JOURNAL OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 30, Number 4, October 2017, Pages 915–958
http://dx.doi.org/10.1090/jams/866
Article electronically published on August 19, 2016

THE DISTRIBUTION OF SANDPILE GROUPS OF RANDOM GRAPHS

MELANIE MATCHETT WOOD

1. Introduction

Given a graph Γ, there is a naturally associated abelian group S_Γ, which has gone in the literature by many names, including the sandpile group, the Jacobian, the critical group, and the Picard group (due to its independent appearance in many subjects ranging from statistical mechanics to combinatorics to arithmetic geometry). The order of S_Γ is the number of spanning trees of Γ. In [Lor08, Section 4], Lorenzini asked about certain statistics of the distribution of group structures among sandpile groups of random graphs. In [CLP13], Clancy, Leake, and Payne noticed that sandpile groups did not appear to be distributed according to the well-known Cohen-Lenstra heuristics [CL84] (which provide a natural first guess as to how random finite abelian groups might be distributed). They conjectured certain new heuristics would govern how often various abelian groups appear as sandpile groups. In this paper, we prove the distribution is as they conjectured.

For $0 < q < 1$, we let $\Gamma \in G(n, q)$ be an Erdős-Rényi random graph on n vertices with independent edge probabilities q. One might first ask, for a finite abelian group G, what is $\lim_{n\to\infty} \mathbb{P}(S_\Gamma \simeq G)$? In fact, as we prove in this paper (Corollary 9.3),

$$\lim_{n\to\infty} \mathbb{P}(S_\Gamma \simeq G) = 0,$$

showing this is too fine a question. We normalize by asking a coarser question about S_Γ. For example, the sandpile group of Γ is asymptotically almost never $\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/11\mathbb{Z}$, but we ask, for example, how often is its 3-part $\mathbb{Z}/3\mathbb{Z}$? A finite abelian group G is simply the direct sum of its Sylow p-subgroups. Let $S_{\Gamma,p}$ be the Sylow p-subgroup of S_Γ. For a fixed prime p, we determine and prove how often (asymptotically) $S_{\Gamma,p}$ is a particular finite abelian p-group G.

Theorem 1.1. *Let p be a prime and G a finite abelian p-group. Then for a random graph $\Gamma \in G(n, q)$, with $S_{\Gamma,p}$ the Sylow p-subgroup of its sandpile group,*

$$\lim_{n\to\infty} \mathbb{P}(S_{\Gamma,p} \simeq G) = \frac{\#\{\textit{symmetric, bilinear, perfect } \phi : G \times G \to \mathbb{C}^*\}}{|G||\operatorname{Aut}(G)|} \prod_{k\geq 0}(1 - p^{-2k-1}). \tag{1}$$

Received by the editors October 21, 2014 and, in revised form, April 21, 2016, July 6, 2016, and July 17, 2016.

2010 *Mathematics Subject Classification.* 05C80, 15B52, 60B20.

This work was done with the support of an American Institute of Mathematics Five-Year Fellowship, a Packard Fellowship for Science and Engineering, a Sloan Research Fellowship, and National Science Foundation grants DMS-1147782 and DMS-1301690.

Theorem 1.1 can be viewed as a result in combinatorics about random graphs, or alternatively viewed as a result in arithmetic statistics (given the analogies to Jacobians of curves over finite fields, both philosophical and precise in terms of component groups of Neron models, discussed in Section 1.1). However, behind Theorem 1.1 is a new universality result on random matrices (see, e.g., Theorem 1.3), showing that certain statistics of random symmetric matrices are quite robust and insensitive to the distribution of the matrices. The methods developed to prove this result include inverse Littlewood-Offord theorems over finite rings and new techniques for studying homomorphisms of finite abelian groups with not only precise structure but also approximate versions of that structure.

Note the product on the right in (1) does not involve G and plays the role of a normalization constant. Also, the entire right-hand side of (1) does not depend on q, the edge-probability of the random graph. If $G = \bigoplus_i \mathbb{Z}/p^{\lambda_i}\mathbb{Z}$ with $\lambda_1 \geq \lambda_2 \geq \cdots$ and μ is the transpose of the partition λ, then we can express the fraction on the left very concretely as

$$\frac{\#\{\text{symmetric, bilinear, perfect } \phi : G \times G \to \mathbb{C}^*\}}{|G||\operatorname{Aut}(G)|} = p^{-\sum_i \frac{\mu_i(\mu_i+1)}{2}} \prod_{i=1}^{\lambda_1} \prod_{j=1}^{\lfloor \frac{\mu_i - \mu_{i+1}}{2} \rfloor} (1-p^{-2j})^{-1} \tag{2}$$

(see Lemmas 7.2 and 7.3). For large p, every factor other than the leading power of p is near 1. For example, if $G = \mathbb{Z}/p^r\mathbb{Z}$, the right-hand side of Theorem 1.1 is $\approx p^{-r}$. If $G = (\mathbb{Z}/p\mathbb{Z})^r$, the right-hand side of Theorem 1.1 is $\approx p^{-r(r+1)/2}$. This explains why cyclic groups are seen as sandpile groups so much more often than higher rank groups of the same size. For example, the Sylow 7-subgroup of a sandpile group is $\mathbb{Z}/49$ about 7 times as often as it is $(\mathbb{Z}/7\mathbb{Z})^2$.

In fact, we show quite a bit more than Theorem 1.1. In particular (see Corollary 9.2) for any finite set of primes we give the asymptotic probabilities of particular Sylow subgroups at all of those primes, and we find that the Sylow subgroups at different primes behave (asymptotically) independently.

To prove Theorem 1.1, we first prove a complete set of moments for the random groups S_Γ. Let $\operatorname{Sur}(A, B)$ denote the set of surjective homomorphisms from A to B.

Theorem 1.2. *Let $G = \bigoplus_{i=1}^r \mathbb{Z}/a_i\mathbb{Z}$ be a finite abelian group with $a_r|a_{r-1}|\cdots|a_1$. Then for a random graph $\Gamma \in G(n,q)$, with S_Γ its sandpile group,*

$$\lim_{n\to\infty} \mathbb{E}(\#\operatorname{Sur}(S_\Gamma, G)) = \prod_i a_i^{i-1}.$$

The product $\prod_i a_i^{i-1}$ occurs as $|\wedge^2 G|$. We refer to $\mathbb{E}(\#\operatorname{Sur}(S_\Gamma, G))$ as the G-*moment* of S_Γ. For comparison, if H is a random group drawn according to the Cohen-Lenstra heuristics, then for all finite abelian groups G the G-moment of H is 1 [CL84, Proposition 4.1(ii) and Corollary 3.7(i)] (see also [EVW16, Section 8]), whereas in our case the G-moments depend on the group G. We also obtain an exponentially decreasing (in n) error term (see Theorem 6.2) for Theorem 1.2.

We then show (in Section 8) that the moments in Theorem 1.2 determine the distribution as given in Theorem 1.1, despite the moments' growing too fast to use the usual probabilistic methods to show that moments determine a unique

distribution. We also deduce many other statistics of sandpile groups of random graphs, including the distribution of their p-ranks (see Corollaries 9.1 and 9.4). For example, the probability that p divides $|S_\Gamma|$ goes to $1 - \prod_{k\geq 0}(1 - p^{-2k-1})$. Even more concretely, the probability that a random graph $\Gamma \in G(n, q)$ has an even number of spanning trees goes to $\approx .5806$. We conclude in Corollary 9.5 that the probability that S_Γ is cyclic is asymptotically at most

$$\zeta(3)^{-1}\zeta(5)^{-1}\zeta(7)^{-1}\zeta(9)^{-1}\zeta(11)^{-1}\cdots \approx .7935212,$$

where ζ is the Riemann zeta function, differing from a conjectured value [Wag00, Conjecture 4.2], and in Corollary 9.6 that the probability that the number of spanning trees of Γ is square-free is asymptotically at most $\zeta(2)^{-1}\zeta(3)^{-1}\zeta(5)^{-1}\zeta(7)^{-1}\zeta(9)^{-1}\cdots \approx .48240306$, again differing from a conjectured value [Wag00, Conjecture 4.4]. See also [Lor08, Section 4] for some questions and results on the topic of how often the sandpile group of a graph is cyclic.

1.1. **Sandpile groups.** For a general introduction to sandpile groups and some beautiful pictures of sandpiles, see the Notices' "What is ... a sandpile?" [LP10]. There is also an overview given in [NW11] of the way the group has arisen in various contexts. One convenient definition is that S_Γ is the cokernel of the reduced Laplacian Δ_Γ of Γ (see [Lor90] and also Section 2.2). Thus $|S_\Gamma| = |\operatorname{Det}(\Delta_\Gamma)|$, which is the number of spanning trees of Γ by Kirchhoff's matrix tree theorem.

The name "sandpile" comes from work studying the dynamics of a sandpile, which is a situation in which there is a number of chips at each vertex of a graph, and a vertex with at least as many chips as its degree can topple, giving a chip to each of its neighbors. (This is also called a chip-firing game, as originally studied in [BLS91].) If chips randomly fall on vertices of a graph, toppling whenever possible, then the recurrent states in this Markov chain naturally form a group (the sandpile group) that is intimately related to the dynamics of the sandpile. This sandpile model was first studied in statistical physics in 1988 [BTW88] (see also [Dha90, Gab93a, Gab93b, Big99]). The sandpile group is also related to the Tutte polynomial of the graph. A generating function for counting elements of the sandpile group, as recurrent sandpiles, by their number of chips (on non-sink vertices) is given by $T(1, y)$, where T is the Tutte polynomial [L97, Gab93a, Gab93b]. See [HLM$^+$] for a survey of some of these aspects of sandpiles.

In an analogy between Riemann surfaces and graphs, the sandpile group has been studied and called the Jacobian (or Picard group or critical group) of the graph [BdlHN97, Big97]. In this context, the group is a discrete analog of the Jacobian of a Riemann surface, or alternatively, an analog of the Jacobian of an algebraic curve over a finite field. In fact, this latter analogy can be made precise, and the group of components of the Néron model of a Jacobian of a curve over a local field is given as a Jacobian of a graph [Lor89, BL02]. In this analogy, the order of the sandpile group appears in the "analytic class number formula" for graphs [HST06], and versions of Riemann-Roch and the Riemann-Hurwitz formulas are known for the Jacobian of graphs [BN07, BN09].

In part motivated by these many connections, the sandpile group has also been studied as an interesting invariant of graphs in its own right and determined for many families of graphs (see the Introduction to [AV12] for pointers to some of this vast literature).

1.2. **Why those probabilities: The relation to the Cohen-Lenstra heuristics.** Some experts had speculated that sandpile groups of random graphs might satisfy a Cohen-Lenstra heuristic. The Cohen-Lenstra heuristics [CL84] were developed to predict the distribution of ideal class groups of quadratic number fields, which are finite abelian groups that measure the failure of unique factorization in quadratic rings of algebraic integers such as $\mathbb{Z}[\sqrt{-5}]$. The basic principle is that a finite abelian group G should occur with probability proportional to $|\operatorname{Aut}(G)|^{-1}$, barring any known bias in how groups appear. It is a well-known phenomenon that objects often occur inversely proportionally to their number of automorphisms. As in our case, with this heuristic, each group must appear with probability 0 because the sum of $|\operatorname{Aut}(G)|^{-1}$ over all finite abelian groups is infinite, but as in this paper, the usual approach is to study the occurrence of a given Sylow p-subgroup G, which is expected to occur with *positive* probability proportional to $|\operatorname{Aut}(G)|^{-1}$.

As a first guess, this is a good one, and in fact the expected value given in Theorem 1.2 when G is cyclic agrees with the average from the Cohen-Lenstra distribution, as was noticed empirically in [CLK+14]. But higher averages do not agree with those from the Cohen-Lenstra distribution. The Cohen-Lenstra distribution has been generalized to many other distributions where there is some additional feature of the relevant finite abelian group. Even in the original Cohen-Lenstra paper [CL84], they modified the heuristic to predict the distribution of Sylow p-subgroups of class groups of real quadratic and higher degree abelian number fields for "good" primes p. Gerth [Ger87a, Ger87b] gave different heuristics to predict the distribution for "bad primes." Cohen and Martinet gave different heuristics that predict the class groups of any kind of extension of any number field [CM90]. New heuristics have been suggested by Malle [Mal08, Mal10] and Garton [Gar12] to replace Cohen and Martinet's heuristics when there are roots of unity in the base field. (Note that our moments in Theorem 1.2 agree with the "$q = 1$ case" of the moments in [Gar12, Corollary 3.1.2], where the quotes are because the work in [Gar12] is motivated by work over a function field over $\mathbb{F}_q$.) Most closely related to the situation for sandpile groups are Delaunay's heuristics for the distribution of Tate-Shafarevich groups of elliptic curves [Del01] (see also [BKLj+13]). These groups are abelian and conjecturally finite, and if finite have a non-degenerate, alternating, bilinear pairing. So Delaunay formulated heuristics that replaced $\operatorname{Aut}(G)$ with automorphisms of G that preserve the pairing.

In fact, the sandpile group comes with a canonical perfect, symmetric, bilinear pairing (see [Lor00, BL02, Sho10]), and so Clancy, Leake, and Payne [CLP13] guessed that this pairing should play a role in the distribution. They conjectured, based on their empirical results, that a particular group G with pairing $\langle , \rangle$ should appear with probability proportional to $|G|^{-1}|\operatorname{Aut}(G, \langle , \rangle)|^{-1}$. Unlike the situation for alternating pairings, where each isomorphism class of group has a unique isomorphism type of pairing, there are many isomorphism types of symmetric pairings, especially for 2-groups. The right-hand side of Theorem 1.1 is what we obtain when summing the heuristic of [CLP13] over all pairings for a given group. It would be very interesting to have a refinement of Theorem 1.1 that determines how often the various pairings occur for each group, and in particular to see if they indeed agree with the prediction of [CLP13].

1.3. **Connections to random matrices.** When Γ is a random graph, the reduced Laplacian Δ_Γ is a random matrix, so one naturally arrives at a question of

statistics of random matrices with integer coefficients. It is a well-studied phenomenon in the field of random matrices that certain statistics of random matrices, e.g., their eigenvalue distributions, are (asymptotically) universal in the sense that they are the same for a large class of different kinds of random matrices. Usually within this class of random matrices, there are some coming from particularly symmetric distributions for which the statistics can be computed much more easily than in the general case. For example, in 1967 Mehta [Meh67] found the eigenvalue distribution of (properly normalized) independent and identically distributed (i.i.d). Gaussian random matrices converges to the uniform distribution on the unit disk. Many authors including Girko [Gir84, Gir04], Bai [Bai97], Bai and Silverstein [BS10], Götze and Tikhomirov [GT06, GT10], Pan and Zhou [PZ10], and Tao and Vu [TV08, TV10] have proven that large classes of i.i.d. random matrices give the same asymptotic eigenvalue distribution, with the most general result [TV10] of this *circular law* requiring no other hypotheses other than mean 0 entries and normalization. There is a similar story for symmetric or Hermitian random matrices [Wig58, Pas72, BS10].

Here, the statistics of interest for our random integral matrices are the distributions of the Sylow p-subgroups of their cokernels. Since for an $n \times n$ matrix of rank r mod p, the cokernel has p-rank $n-r$, the cokernel statistics are a refinement of rank mod p statistics. In [CLK$^+$14], Clancy, Leake, Kaplan, Payne, and the current author show that for a random symmetric matrix over the p-adic integers $\mathbb{Z}_p$, drawn with respect to Haar measure, the cokernels are distributed as in Theorem 1.1. These matrices drawn with respect to Haar measure should be seen as the analog of Gaussian random matrices in the circular law story above—they are drawn from a distribution with the most possible symmetry and thus make computations more accessible. For (not necessarily symmetric) matrices, the work of Freidman and Washington [FW89] showed that cokernels of random matrices over $\mathbb{Z}_p$, drawn with respect to Haar measure, are distributed according to the Cohen-Lenstra heuristics. (See also [BKLj$^+$13] for the case of alternating Haar random matrices.)

Now we naturally ask whether these asymptotic cokernel (and rank mod p) distributions for the nicest (Haar) random matrices are *universal* in the sense that they hold more robustly for many different kinds of random matrices, as with eigenvalue statistics in the circular law. There is work (with some errors) of Maples [Map13] on this problem for (not necessarily symmetric) matrices with i.i.d. entries in $\mathbb{Z}_p$. In this paper we prove the following strong universality result for cokernel (and rank mod p) distributions of symmetric random matrices.

Theorem 1.3. *Let $0 < \alpha < 1$ be a real number and p be a prime. Let X be a symmetric random matrix in $M_{n\times n}(\mathbb{Z})$ with entries X_{ij} independent for $i \le j$ such that for any $t \in \mathbb{Z}/p\mathbb{Z}$, the probability $\mathbb{P}(X_{ij} \equiv t \pmod p) \le 1-\alpha$. Let $\operatorname{col}(X)$ denote the column space of X in $\mathbb{Z}^n$ and $\operatorname{cok} X_p$ denote the Sylow p-subgroup of $\mathbb{Z}^n/\operatorname{col}(X)$. For any finite abelian p-group G,*

$$\lim_{n\to\infty} \mathbb{P}(\operatorname{cok} X_p \simeq G) = \frac{\#\{\textit{symmetric, bilinear, perfect } \phi : G \times G \to \mathbb{C}^*\}}{|G||\operatorname{Aut}(G)|} \prod_{k\ge 0}(1-p^{-2k-1})$$

and

$$\lim_{n\to\infty} \mathbb{P}(\text{rank}(\ X \bmod p) = n - r) = p^{-\frac{r(r+1)}{2}} \prod_{i=r+1}^{\infty} (1-p^{-i}) \prod_{i=1}^{\infty} (1-p^{-2i})^{-1}.$$

Theorem 1.3 is proven in the same way as Corollaries 9.2 and 9.4 (see Remark 9.7). We also prove asymptotic independence of the joint distribution for finitely many primes p (see Corollary 9.2). In Theorem 1.1, our random matrix is a graph Laplacian, so it does not have independent entries, and we further work to show universality even given the dependence of the diagonal.

The $r = 0$ case of the second part of Theorem 1.3 gives the probability that X mod p is non-singular. The singularity probability of random matrices has been well studied over $\mathbb{R}$ and over $\mathbb{F}_p$. Over $\mathbb{R}$, upper bounds on the singularity probability of a random matrix with ± 1 i.i.d. entries have been given by Komlós [Kom67, Kom68], Kahn, Komlós, and Szemerédi [KKS95], Tao and Vu [TV06, TV07], and the current best bound (and extension to more general entry distributions) is due to Bourgain, Vu, and P. M. Wood [BVW10]. Over $\mathbb{F}_p$, there is work determining the asymptotic singularity probability for quite general random matrices over $\mathbb{F}_p$ by a large number of authors, including Kozlov [Koz66], Balakin [Bal68], Kovalenko and Levitskaya [KL75], Kovalenko, Levitskaya, and Savchuk [KLS86], Brent and McKay [BM87], Charlap, Rees, and Robbins [CRR90], Blömer, Karp, and Welzl [BKW97], Cooper [Coo00], Kahn and Komlós [KK01], and Maples [Map10].

Our matrices Δ_Γ are symmetric, which adds significant difficulty over the case of independent entries. In the case of singularity probability of symmetric matrices over $\mathbb{R}$ with independent entries on and above the diagonal, Costello, Tao, and Vu obtained the first good upper bound [CTV06], with improvements by Costello [Cos13] and Nguyen [Ngu12], and the current best bound due to Vershynin [Ver11]. To our knowledge, this paper is the first work that addresses the singularity probability of random symmetric matrices over $\mathbb{F}_p$. The specific tools we develop to prove our results are new and of a more algebraic flavor than the previous work on singularity probability over $\mathbb{R}$ or $\mathbb{F}_p$, but many themes, including inverse Littlewood-Offord theorems, are similar.

1.4. **Our method to determine the moments.** We prove Theorem 1.2 via a result in which a much more general random symmetric matrix replaces the graph Laplacian (see Theorem 6.1). We then prove (in Theorem 8.2) that these moments in fact determine a unique distribution. We are thus able to use the case of cokernels of *uniform* random symmetric matrices over $\mathbb{Z}/a\mathbb{Z}$, whose distributions were determined in [CLK+14], and by our universality results, deduce that the moments and distribution of this simple case hold in great generality.

There are some interesting features of our method, in particular in comparison to previous work. First of all, we only have to consider linear Littlewood-Offord problems, and not quadratic ones (as in [CTV06, Cos13, Ngu12, Ver11]), even though our matrices are symmetric. Second, our method can easily handle the dependence of the diagonal of the Laplacian on the rest of the entries. Third, we in fact obtain the moments, which are interesting averages in their own right and have been studied at length for finite abelian group valued random variables in the work related to the Cohen-Lenstra heuristics. (For example, Davenport and Heilbronn [DH71] determined the $\mathbb{Z}/3\mathbb{Z}$-moment of the class groups of quadratic fields. See also [Bha05, EVW16, EVW12, FK06, FK07, Gar12] for other examples of results in

number theory about certain G-moments of class groups.) Fourth, the moments only depend on the reduction of the matrix entries from $\mathbb{Z}$ to $\mathbb{Z}/a\mathbb{Z}$ for some a, so we are able to work with random symmetric matrices over $\mathbb{Z}/a\mathbb{Z}$. (Of course, we need all the moments, so we must work over $\mathbb{Z}/a\mathbb{Z}$ for each a.)

Theorem 1.2 gives the expected number of surjections $S_\Gamma \to G$. The sandpile group is $S_\Gamma = \mathbb{Z}^{n-1}/\Delta_\Gamma\mathbb{Z}^{n-1}$, so it suffices to determine to probability that a surjection $F : \mathbb{Z}^{n-1} \to G$ descends to S_Γ (for each F). Equivalently, we determine the probability that $F\Delta_\Gamma = 0$. This is a system of linear equations in the entries of Δ_Γ. The system is generated by on the order of n equations and is in $\binom{n}{2}$ variables. (This contrasts with the usual Littlewood-Offord problem which is 1 equation in n variables.) Unfortunately, the natural generators for this system have only order n of the $\binom{n}{2}$ coefficients non-zero. The system of equations is parametrized by $\mathrm{Hom}(\mathbb{Z}^{n-1}, G^*) = (G^*)^{n-1}$, where G^* is the group of characters on G. Further, some nontrivial $C \in (G^*)^{n-1}$ (we call these *special*) turn out to give equations in which *all* of the coefficients are 0, and which C are special depends on the choice of F.

So while we have linear Littlewood-Offord type problems over $\mathbb{Z}/a\mathbb{Z}$ (with a not necessarily prime, and with a growing number of linear equations instead of a single equation), the difficulty is to understand what structural properties of F and C influence how many of the coefficients of these equations are 0 (see Section 3). Our results are inverse Littlewood-Offord theorems (e.g., see Lemma 4.1) in the sense that they say that any F that does not obey a desired bound has some very specific structure that we use to give an upper bound on the number of bad F. We develop two new concepts, *depth* and *robustness*, to capture these relevant kinds of structure. We will give a brief overview of these concepts now; full details are included as the concepts arise in the paper.

For $\sigma \subset [n-1]$, let V_σ denote the column vectors in $\mathbb{Z}^{n-1}$ that have σ entries 0. *Depth* captures the structural properties of F that influence how many non-zero coefficients appear in our system of equations. For an integer D with prime factorization $\prod_i p_i^{e_i}$, let $\ell(D) = \sum_i e_i$.

Definition. The *depth* (depending on a parameter $\delta > 0$) of a surjection $F : \mathbb{Z}^{n-1} \to G$ is the maximal positive D such that there is a $\sigma \subset [n-1]$ with $|\sigma| < \ell(D)\delta(n-1)$ such that $D = [G : FV_\sigma]$, or is 1 if there is no such D.

The idea is that up to ignoring a small number of basis vectors (those corresponding to σ), the image of F is index D in G. For the σ in the definition of depth, the group FV_σ can be thought of as the "stable" image of F.

Robustness captures the structural properties of C that influence how many non-zero coefficients appear in a particular equation, given F. Viewing $F \in \mathrm{Hom}(\mathbb{Z}^{n-1}, G)$ and $C \in \mathrm{Hom}(\mathbb{Z}^{n-1}, G^*)$, we can add them to obtain $F + C \in \mathrm{Hom}(\mathbb{Z}^{n-1}, G \oplus G^*)$.

Definition. Given F, we say C is *robust* for F (depending on a parameter $\gamma > 0$), if for every $\sigma \subset [n-1]$ with $|\sigma| < \gamma(n-1)$,

$$\ker(F + C|_{V_\sigma}) \neq \ker(F|_{V_\sigma}).$$

We can think of a robust C somewhat intuitively as preserving more information about V than F does, even up to ignoring a small number of basis vectors. Unfortunately, it is not easy to see why this controls non-zero coefficients without getting into the technical details.

We identify the special C exactly in terms of F. Despite their rarity, the special C give the limit in Theorem 1.2 (the main term in Theorem 6.2). The remaining cases form a complicated error term that we must bound. For F of depth 1, for non-special C we prove the associated equation has at least order of n non-zero coefficients, and for robust C we prove the associated equation has at least order of n^2 non-zero coefficients. For each larger depth, we compare F to a combination of a depth 1 "F" for a subgroup FV_σ of G (where we use the above) and an "F" for a quotient group G/FV_σ of G (where we use an Odlyzko-type bound). There is a delicate balance between the number of non-zero coefficients we can get in each case and the number of pairs (F, C) that fall into that case.

Finally, to deal with the dependence of the diagonal in Δ_Γ, we actually do all of the above for a matrix with independent diagonal entries and then enlarge F to condition on what we require of the diagonal.

1.5. **Our method to determine the distribution from the moments.** The question of when the moments of a distribution determine a unique distribution is well-studied in probability and called the moment problem. Roughly, if the sequence of moments of a random variable does not grow too fast, then the distribution of the random variable is determined by the moments. For example, Carleman's condition states that if $\sum_{k=1}^{\infty} m_{2k}^{-1/(2k)}$ diverges, then there is a unique distribution on $\mathbb{R}$ having m_k as the kth moment [Dur07, Section 2.3e]. The standard counterexample is based on the lognormal density and has kth moment $e^{k^2/2}$. In particular, there are many $\mathbb{R}$-valued random variables X with distinct distributions, such that for every k, we have $\mathbb{E}(X^k) = e^{k^2/2}$.

In our problem, the moments grow like the lognormal counterexample. One can see this even if we were only interested in the p-ranks of sandpile groups. Recall our moments are indexed by groups, but we will compare some of them to a usual moment. Note that $\#\operatorname{Hom}(S_\Gamma, (\mathbb{Z}/p\mathbb{Z})^k) = X^k$ for $X = p^{p\text{-rank}(S_\Gamma)}$. By adding Theorem 1.2 over all subgroups G of $(\mathbb{Z}/p\mathbb{Z})^k$ we conclude $\mathbb{E}(X^k)$ is of order $p^{(k^2-k)/2}$. However, the fact that our random variable X can only take values in powers of p makes the problem of recovering the distribution not completely hopeless.

If we were interested just in p-ranks (and did not want to distinguish between $\mathbb{Z}/p\mathbb{Z}$ and $\mathbb{Z}/p^2\mathbb{Z}$ for example), we could apply a method of Heath-Brown [HB94a, Lemma 17]. His strategy can be used to show that if X is a random variable valued in $\{1, p, p^2, \dots\}$, and there is a constant C such that for all integers $k \geq 0$ we have $\mathbb{E}(X^k) \leq Cp^{k^2/2}$, then the distribution of X is determined by its moments. Heath-Brown uses coefficients of precisely constructed analytic functions of one variable to lower-triangularize the infinite system of equations given by the moments. (See also [FK06, Section 4.2] which has a similar result but with a method that does not generalize to suit our needs.)

In order to recover the distribution of the entire Sylow p-subgroups of the sandpile group, we develop a generalization of Heath-Brown's method that replaces the analytic functions of one variable with analytic functions of several complex variables. However, the straightforward generalization which uses Heath-Brown's functions for each variable is too weak for our purposes. We perfectly optimize a function in each variable for our needs, and our moments are *just* small enough for it to work. In the end, we prove that mixed moments determine a unique joint

distribution in cases where, as above, the moments are growing too fast to use Carleman's condition but where we have a restriction on the values taken by the random variables.

1.6. **Further questions.** This work raises many further questions. While we obtain an error bound in n for Theorem 1.2 (see Theorem 6.2), we have not made explicit the dependence of the constant in that error bound on G. It would be interesting to know if such an explicit dependence could translate into an error bound in n for Theorem 1.1, and of what size.

We also work with p fixed, and therefore our methods are not ideal for questions that require consideration of p large compared to n, such as determining the probability that S_Γ is cyclic (for which we obtain only an upper bound, though at what, in light of our results, seems very likely to be the correct answer). It would be very interesting to know if our approach could be combined with ideas from [Map13], which are uniform in p, to determine the probability that S_Γ is cyclic. As a by-product of understanding the group structure, we have determined the distribution of the size of $|S_\Gamma|$ in the p-adic metric, but it is also natural to ask about the distribution of $|S_\Gamma|$ as a real number. While from the above we see that it is any particular size with asymptotic probability 0, we can ask about the probability that it lies in appropriately sized intervals. As discussed above, it would also be nice to have results on the distribution of the pairing on S_Γ.

Another interesting question is whether results such as Theorems 1.1 and 1.2 hold for other models of random graphs or whether the values of the probabilities and the moments change (see [CLK$^+$14, Remark 2]). Our results already allow the edge probabilities to vary as long as they are independent and bounded above and below by a constant. However, it would be interesting to know if one obtains the same distribution on sandpile groups for sparser graphs, in particular in the case of $G(n, q)$ when $q \geq (1 + \epsilon) \log(n)/n$ in which the graph is still asymptotically almost surely connected. There is an analogous question for denser graphs (and if q gets too large, the graphs will be too close to complete graphs and will definitely not follow the distribution of Theorem 1.1). It would also be interesting to determine the distribution of sandpile groups of r-regular graphs.

In this paper we work with random symmetric matrices as the basic object, and we have already had to deal with one kind of dependency (beyond the symmetry) in our matrices—the dependency of the diagonal in the graph Laplacian on the other entries. We specifically developed our method to handle this dependency easily, and it should be able to handle other linear dependencies on the columns of a symmetric matrix as well, as long as they apply to all the columns. It would be nice to understand whether our approach can be extended to handle linear dependencies that only apply to some of the columns, and in general to what extent dependencies affect the outcome of the distribution of the cokernels of random symmetric matrices. Another interesting case to consider is one in which some of the entries of the matrix are fixed, such as for the adjacency matrix of a random graph in which case the diagonal entries are 0. The cokernel of the adjacency matrix is called the *Smith group* and has been studied, e.g., in [CSX14, DJ13].

In this paper, our method finds the actual values of the probabilities occurring in Theorem 1.1 by using our universality results that say the values are the same for a large class for random matrices, and then citing a computation for the case of uniform random symmetric matrices over $\mathbb{Z}/a\mathbb{Z}$. There are further statistics

of these uniform random matrices over $\mathbb{Z}/a\mathbb{Z}$, which if determined would, using our Corollary 9.1, immediately give more statistics of sandpile groups of random graphs. See the end of Section 9 for details.

1.7. **Outline of the paper.** In Sections 3 through 6 we prove Theorem 1.2 (and the analog of Theorem 1.2 for cokernels of symmetric random matrices). In Section 8, we prove that the moments of Theorem 1.2 in fact determine the relevant distributions. In Section 9, we show what those distributions are, by comparing to the case of cokernels of uniform random symmetric matrices over $\mathbb{Z}/a\mathbb{Z}$, for which the distribution and the moments have already been computed in [CLK+14]. In particular, we deduce Theorem 1.1 from Corollary 9.2.

2. Background

2.1. **Cokernels of matrices.** For an $n \times n$ matrix M with entries in a ring R, let $\mathrm{col}(M)$ denote the column space of M (i.e., the image of the map $M : R^n \to R^n$). We define the *cokernel* of M,

$$\mathrm{cok}(M) := R^n / \mathrm{col}(M).$$

2.2. **Sandpile group.** Let $[n]$ denote the set $\{1, \ldots, n\}$. Let Γ be a graph on n vertices labeled by $[n]$. The Laplacian L_Γ is an $n \times n$ matrix with (i, j) entry

$$\begin{cases} 1 \text{ if } \{i, j\} \text{ is an edge of } \Gamma \\ 0 \text{ if } i \neq j \text{ and } \{i, j\} \text{ is not an edge of } \Gamma \\ -\deg(i) \text{ if } i = j. \end{cases}$$

We have that L_Γ is a matrix with coefficients in $\mathbb{Z}$. Let $Z \subset \mathbb{Z}^n$ be the vectors whose coordinates sum to 0. Clearly, $\mathrm{col}(L_\Gamma) \subset Z$. We define the sandpile group $S_\Gamma := Z/\mathrm{col}(L_\Gamma)$. This is clearly a finitely generated abelian group, and it is finite if and only if Γ is connected.

2.3. **Random graphs.** We write $\Gamma \in G(n, q)$ to denote that Γ is an Erdős-Rényi random graph on n labeled vertices with each edge independent and occurring with probability q.

2.4. **Finite abelian groups.** For a prime p, a finite abelian p-group is isomorphic to $\bigoplus_{i=1}^{r} \mathbb{Z}/p^{\lambda_i}\mathbb{Z}$ for some positive integers $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_r$. We call the partition λ the *type* of the abelian p-group. For a partition λ, we use G_λ to denote a p-group of type λ when p is understood.

For an $a \in \mathbb{Z}$ and a finite abelian group G, we can form the *tensor product* $G \otimes_{\mathbb{Z}} \mathbb{Z}/a\mathbb{Z}$. This is a tensor product of the two objects as $\mathbb{Z}$-modules, but it is particularly simple to say what it does to a particular group. We have

$$\left(\bigoplus_i \mathbb{Z}/a_i\mathbb{Z} \right) \otimes_{\mathbb{Z}} \mathbb{Z}/a\mathbb{Z} = \bigoplus_i \mathbb{Z}/(a_i, a)\mathbb{Z},$$

where (a_i, a) is the greatest common divisor of a_i and a. So for primes $p \nmid a$, the Sylow p-subgroups are killed, and if p^e is the highest power of a prime p dividing a, then summands $\mathbb{Z}/p^i\mathbb{Z}$ of G for $i \leq e$ are untouched and summands $\mathbb{Z}/p^i\mathbb{Z}$ for $i > e$ are changed to $\mathbb{Z}/p^e\mathbb{Z}$. In terms of the partition diagram for the type λ of the Sylow p-subgroup of G, it is truncated so that all rows are length at most e.

The *exterior power* $\wedge^2 G$ is defined to be the quotient of $G \otimes G$ by the subgroup generated by elements of the form $g \otimes g$. If G_p are the Sylow p-subgroups of G, then $\wedge^2 G = \bigoplus_p \wedge^2 G_p$. If G_p is type λ, generated by e_i with relations $p^{\lambda_i} e_i = 0$, then $\wedge^2 G_p$ is generated by the $e_i \wedge e_j$ for $i < j$ with relations $p^{\lambda_j} e_i \wedge e_j = 0$. So

$$\wedge^2 G_p \simeq \bigoplus_i (\mathbb{Z}/p^{\lambda_i}\mathbb{Z})^{i-1}.$$

For a partition λ, let λ' be the *transpose partition*, so λ'_j is the number of λ_i that are at least j. Note that $\sum_i (i-1)\lambda_i$ is the sum over boxes in the partition diagram of λ of $i-1$, where i is in the row the box appears in. Summing by column, we obtain $\sum_i (i-1)\lambda_i = \sum_j \frac{\lambda'_j(\lambda'_j-1)}{2}$. Of particular importance to us will be the size

$$|\wedge^2 G_p| = p^{\sum_i (i-1)\lambda_i} = p^{\sum_j \frac{\lambda'_j(\lambda'_j-1)}{2}}.$$

The exponent of a finite abelian group is the smallest positive integer a such that $aG = 0$. When $R = \mathbb{Z}/a\mathbb{Z}$, any finite abelian groups H, G of exponent dividing a are also *R-modules*, and their group homomorphisms are the same as their R-module homomorphisms. When the ring R is understood, we write G^* for $\mathrm{Hom}(G, R)$. If the exponent of G divides a, then G^* is non-canonically isomorphic to G.

We use $\langle g_1, \ldots, g_m \rangle$ to denote the subgroup generated by $g_1, \ldots, g_m$.

2.5. **Pairings.** A map $\phi : G \times G \to \mathbb{C}^*$ is symmetric if $\phi(g,h) = \phi(h,g)$ for all $g, h \in G$. When G is an abelian group, the map ϕ is bilinear if for all $g_1, g_2, h \in G$ we have $\phi(g_1 + g_2, h) = \phi(g_1, h)\phi(g_2, h)$, and similarly for the right factor. The map ϕ is perfect if the only $g \in G$ with $\phi(g, G) = 1$ is $g = 0$, and similarly for the other factor.

2.6. **Notation.** We denote the order of groups and sets using either absolute value signs $|\cdot|$ or $\#$. (This inconsistency is because sometimes the absolute value signs are confusing when coupled with the notation $|$ for "divides" or parentheses, and the sharps take up too much space in some formulas.) We use $\simeq$ to denote "is isomorphic to." We use $\mathbb{P}$ to denote probability and $\mathbb{E}$ to denote expected value. The letter p will always denote a prime.

3. Obtaining the moments I: Determining the structural properties of the equations

In the next four sections, we will prove Theorem 1.2. Let G be a finite abelian group and $\Gamma \in G(n,q)$. We will write S for S_Γ and L for the Laplacian L_Γ. The group S is defined as a quotient of Z, so any surjection $S \to G$ lifts to a surjection $Z \to G$, so we have

$$\mathbb{E}(\#\,\mathrm{Sur}(S, G)) = \sum_{F \in \mathrm{Sur}(Z,G)} \mathbb{P}(\mathrm{col}(L) \subset \ker(F)).$$

Our approach will be to estimate the probabilities on the right, but we will start with a slightly more general setup.

Let a be a positive integer and let G be a finite abelian group of exponent dividing a. Let R be the ring $\mathbb{Z}/a\mathbb{Z}$. We will retain this notation through Section 6. Note that $\mathrm{Sur}(S, G) = \mathrm{Sur}(S \otimes \mathbb{Z}/a\mathbb{Z}, G)$. Said another way, whether $\mathrm{col}(L) \subset \ker(F)$ only depends on the entries of L modulo a.

In this and the next three sections, we shall do all our "linear algebra" over R. Since R is not a domain, this necessitates working more abstractly instead of just with matrices. A particular source of difficulty compared to the case of linear algebra over a field is that not all exact sequences of R-modules split; i.e., there are subgroups of our finite abelian groups that are not direct summands. We will work carefully to find summands when we need them.

For an R-module A, let $A^* := \mathrm{Hom}(A, R)$. We define the R-module $V = R^n$. We have a distinguished basis $v_1, \dots, v_n$ of V, and a dual basis $v_1^*, \dots, v_n^*$ of V^*. Also let $W = R^n$. We have a basis $w_1, \dots, w_n$ of W, and a dual basis $w_1^*, \dots, w_n^*$ of W^*. If we realize V and W as spaces of length n column vectors with entries in R, then an $n \times n$ matrix M over R gives a homomorphism from W to V, i.e., $M \in \mathrm{Hom}(W, V)$.

Let $F \in \mathrm{Hom}(V, G)$ be a homomorphism.[1] Then $\mathrm{col}(M) \subset \ker(F)$ if and only if the composition $FM \in \mathrm{Hom}(W, G)$ is 0. Let ζ be a primitive ath root of unity. For $M \in \mathrm{Hom}(W, V)$, since FM is in the finite abelian group $\mathrm{Hom}(W, G)$ of order $|G|^n$, the Fourier expansion gives[2]

$$1_{FM=0} = \frac{1}{|G|^n} \sum_{C \in \mathrm{Hom}(\mathrm{Hom}(W,G),R))} \zeta^{C(FM)}.$$

Thus if $X \in \mathrm{Hom}(W, V)$ is a random matrix,

$$\mathbb{P}(FX = 0) = \mathbb{E}(1_{FX=0}) = \frac{1}{|G|^n} \sum_{C \in \mathrm{Hom}(\mathrm{Hom}(W,G),R))} \mathbb{E}(\zeta^{C(FX)}).$$

These C give the equations a matrix that has to satisfy in order for a surjection given by F to extend to the cokernel of the matrix. (Hence, "equations" appears in the title of this section.) As a function of X, we have that $C(FX)$ is a linear function of the entries X_{ij} (for $i \le j$) of the matrix X. Below we will work out explicitly the coefficient of each X_{ij}. When these entries X_{ij} are independent, we can then factor the expected value above (see Equation (3) below).

Since $W \simeq R^n$, we have that the natural map $\mathrm{Hom}(W, R) \otimes G \to \mathrm{Hom}(W, G)$ is an isomorphism. So, the natural map $\mathrm{Hom}(\mathrm{Hom}(W, G), R)) \to \mathrm{Hom}(\mathrm{Hom}(W, R) \otimes G, R))$ is an isomorphism. Composing with the isomorphism $\mathrm{Hom}(W^* \otimes G, R) \simeq \mathrm{Hom}(W^*, \mathrm{Hom}(G, R))$, we have an isomorphism $\mathrm{Hom}(\mathrm{Hom}(W, G), R)) \to \mathrm{Hom}(W^*, G^*)$. Via this isomorphism, we will view[3] $C \in \mathrm{Hom}(W^*, G^*)$. So for $w^* \in W^*$, we have $C(w^*) \in G^*$. We write $e : G^* \times G \to R$ for the map that evaluates a homomorphism.

Because of our interest in random matrices whose entries *with respect to a specific choice of basis of* V are independent, we must necessarily sometimes compute things with respect to this basis. In other parts of the proof, we will work with a different

[1] If we realize V as a space of column vectors of length n, and G as a space of column vectors of length k, then we can realize F as a $k \times n$ matrix. However, note that G will not be the space of *all* length k column vectors over R. If $G = \bigoplus \mathbb{Z}/a_i\mathbb{Z}$, then the ith entry of G (and thus the entries in the ith row of F) must be multiples of a/a_i.

[2] If a is a prime p, and we realize everything as in the footnote above, then FX is a $k \times n$ matrix with entries in $\mathbb{Z}/p\mathbb{Z}$, and the C in the sum are the $\mathbb{Z}/p\mathbb{Z}$-valued functions on $k \times n$ matrices that give linear combinations of the coefficients of the matrix. We could realize each C as $\mathrm{Tr}(\bar{C}-)$ for some $n \times k$ matrix $\bar{C}$ over $\mathbb{Z}/p\mathbb{Z}$.

[3] When a is prime, following the above footnotes, $\bar{C}$ gives the $n \times k$ matrix $\in \mathrm{Hom}(W^*, G^*)$ that we associate to C (and call C, by a slight abuse of notation).

choice of basis more closely aligned with G (through F). For some parts of our proof, in particular because we are working over the non-domain $R = \mathbb{Z}/a\mathbb{Z}$, it will be much simpler to work in a basis-free way.

In particular, our interest is in symmetric matrices X. For this even to make sense, we now identify[4] $W = V^*$, and so $v_i = w_i^*$ and $v_i^* = w_i$. Our matrix X will be symmetric, and so we have

$$\begin{aligned} C(FX) &= \sum_{i=1}^{n}\sum_{j=1}^{n} e(C(v_j), F(v_i))X_{ij} \\ &= \sum_{i=1}^{n}\sum_{j=i+1}^{n} (e(C(v_j), F(v_i)) + e(C(v_i), F(v_j)))X_{ij} + \sum_{i=1}^{n} e(C(v_i), F(v_i))X_{ii}. \end{aligned}$$

We will study these coefficients in detail. For $i < j$ we define, $E(C, F, i, j) := e(C(v_j), F(v_i)) + e(C(v_i), F(v_j))$, and we also define $E(C, F, i, i) := e(C(v_i), F(v_i))$. Thus when the entries X_{ij} (for $i \le j$) of X are independent,

$$\mathbb{P}(FX = 0) = \frac{1}{|G|^n} \sum_{C \in \mathrm{Hom}(\mathrm{Hom}(W,G),R))} \prod_{i \le j} \mathbb{E}(\zeta^{E(C,F,i,j)X_{ij}}). \tag{3}$$

When $u \neq 0$, we will see that $\mathbb{E}(\zeta^{uX_{ij}})$ is pretty small (Lemma 4.2). Thus, our goal is to see that as many as possible of these $E(C, F, i, j)$ coefficients are non-zero, as often as possible. To do this we will have to identify structural properties of F and of C that influence the number of non-zero coefficients. Given F and C, there are on the order of n^2 coefficients, and so ideally we would like on the order of n^2 of them to be non-zero. Unfortunately, given F, this is not the case for every C. Given a "good" F, for most C we will be able to show that on the order of n^2 of the coefficients are non-zero, but for some only on the order of n of the coefficients are non-zero, and for some C all of the coefficients are 0. The rest of this section is devoted to explaining the structural properties of C that will determine which of the three cases above it falls into. (This is all for "good" F. In this section we will determine the structural property that makes F good, and in Section 5 we will come to the rest of the F, which we will have to stratify by further structural properties.)

We will now write these coefficients $E(C, F, i, j)$ more equivariantly via a pairing. For $F \in \mathrm{Hom}(V, G)$ and $C \in \mathrm{Hom}(V, G^*)$, we have a map[5] $\phi_{F,C} \in \mathrm{Hom}(V, G \oplus G^*)$ given by adding F and C. (In the Introduction we called this $F + C$, but that notation would get too cumbersome below.) Similarly, we have a map $\phi_{C,F} \in \mathrm{Hom}(V, G^* \oplus G)$ given by adding C and F. There is a map

$$\begin{aligned} (G \oplus G^*) \times (G^* \oplus G) &\xrightarrow{t} R, \\ ((g_1, \phi_1), (\phi_2, g_2)) &\mapsto \phi_2(g_1) + \phi_1(g_2). \end{aligned}$$

Note that for all $u, v \in V$,

$$t(\phi_{C,F}(u), \phi_{F,C}(v)) = e(C(u), F(v)) + e(C(v), F(u)).$$

[4]We see here another reason using matrices and vectors is problematic. Since V is supposed to consist of column vectors, V^* is naturally row vectors, but yet W is column vectors.

[5]Following the above footnotes, if we have matrices F and $\bar{C}$, then $\phi_{F,C}$ corresponds to the matrix obtained by stacking F on top of $\bar{C}^t$.

Note that V has distinguished submodules V_σ generated by the v_i with $i \notin \sigma$ for each $\sigma \subset [n]$. So V_σ comes from not using the coordinates in σ. Clearly, for any submodule U of V,

$$\ker(\phi_{F,C}|_U) \subset \ker(F|_U).$$

Now we will define the key structural property of C (with respect to F) that determines if enough of the coefficients $E(C, F, i, j)$ are non-zero.

Definition. Let $0 < \gamma < 1$ be a real number which we will specify later in the proof. Given F, we say C is *robust* (for F) if for every $\sigma \subset [n]$ with $|\sigma| < \gamma n$,

$$\ker(\phi_{F,C}|_{V_\sigma}) \neq \ker(F|_{V_\sigma}).$$

Otherwise, we say C is *weak* for F.

We will estimate the number of weak C.

Lemma 3.1 (Estimate for number of weak C)**.** *Given G, there is a constant C_G such that for all n the following holds. Given $F \in \mathrm{Hom}(V, G)$, the number of $C \in \mathrm{Hom}(V, G^*)$ such that C is weak for F is at most*

$$C_G \binom{n}{\lceil \gamma n \rceil - 1} |G|^{\gamma n}.$$

Proof. If C is weak, then there exists some $\sigma \subset [n]$ with $|\sigma| < \lceil \gamma n \rceil$ such that

$$\ker(\phi_{F,C}|_{V_\sigma}) = \ker(F|_{V_\sigma}).$$

If the above equality holds, it will still hold if we enlarge σ, so we can assume $|\sigma| = \lceil \gamma n \rceil - 1$. We note in particular this implies that for $s \in V_\sigma$, we have that Cs is determined by Fs. (If $Fs = Fs'$ but $Cs \neq Cs'$, then $s - s' \in \ker F$ but $s - s' \notin \ker \phi_{F,C}|_{V_\sigma}$.) Let $H := \mathrm{im}\, F|_{V_\sigma}$. Further, there is a homomorphism $\psi : H \to G^*$ so that $Cs = \psi(Fs)$ for all $s \in V_\sigma$. There are $\binom{n}{\lceil \gamma n \rceil - 1}$ choices for σ, then $|G|^{\lceil \gamma n \rceil - 1}$ choices for Cv_i for $i \in \sigma$, then $\#\mathrm{Hom}(H, G^*)$ choices for ψ, and then C is determined. Note that since H is a subgroup of G we can find C_G such that $\#\mathrm{Hom}(H, G^*) \leq C_G$. □

Now we will find a sufficient condition for C to be weak in terms of our pairing t.

Lemma 3.2. *Let $F \in \mathrm{Hom}(V, G)$ and $C \in \mathrm{Hom}(V, G^*)$. Let U be a submodule of V such that $FU = G$. Then if U' is a submodule of V such that t is 0 on $\phi_{C,F}(U) \times \phi_{F,C}(U')$, then the projection map $G \oplus G^* \to G$, when restricted to $\phi_{F,C}(U')$, is an injection. In particular* $\ker(\phi_{F,C}|_{U'}) = \ker(F|_{U'})$.

Proof. Suppose for the sake of contradiction that there is a $k \in U'$ with $Fk = 0$ and $Ck = \psi \neq 0 \in G^*$. Since $\psi \neq 0$, there must be some $g \in G$ such that $\psi(g) \neq 0$. Since $FU = G$, there must be some $r \in U$ such that $Fr = g$. Suppose $Cr = \psi'$. Then $t(\phi_{C,F}(r), \phi_{F,C}(k)) = \psi'(0) + \psi(g) \neq 0$. So, we conclude $\phi_{F,C}(U')$ injects into G.

If $\ker(\phi_{F,C}|_{U'}) \neq \ker(F|_{U'})$, then there is some $(0, \phi) \in \phi_{F,C}(U')$ with $\phi \neq 0$, which is a contradiction. □

Corollary 3.3. *Let $F \in \mathrm{Hom}(V, G)$ and $C \in \mathrm{Hom}(V, G^*)$. Let U be a submodule of V such that $FU = G$. If*

$$\#\{i \in [n] \mid t(\phi_{C,F}(U), \phi_{F,C}(v_i)) \neq 0\} < \gamma n,$$

then C is weak for F.

Proof. Let $\sigma := \{i \in [n] \mid t(\phi_{C,F}(U), \phi_{F,C}(v_i)) \neq 0\}$. Then $t(\phi_{C,F}(U), \phi_{F,C}(V_\sigma)) = 0$, and so by Lemma 3.2 we have that C is weak for F. □

Now we will identify the influential structural property of F (which will make it "good" as discussed above), which is a (transpose and) generalization of the notion of a linear code from vector spaces to R-modules.

Definition. We say that $F \in \mathrm{Hom}(V, G)$ is a *code* of distance w, if for every $\sigma \subset [n]$ with $|\sigma| < w$, we have $FV_\sigma = G$. In other words, F is not only surjective, but would still be surjective if we throw out (any) fewer than w of the standard basis vectors from V. (If a is prime so that R is a field, then this is equivalent to whether the transpose map $F : G^* \to V^*$ is injective and has image $\mathrm{im}(F) \subset V^*$ as a linear code of distance w, in the usual sense.)

We have the following lemma about codes which we will next combine with the property of robustness to get a good bound on the number of $E(C, F, i, j)$ that are non-zero.

Lemma 3.4. *Let H be a finite R-module with Sylow p-subgroup of type λ. Suppose $F \in \mathrm{Hom}(V, H)$ is a* code *of distance δn, and let $C \in \mathrm{Hom}(V, H^*)$. Let $r = \lambda'_1$. Then we can find $A_1, \ldots, A_r \in H$ and $B_1, \ldots, B_r \in H^*$ such that for every $1 \leq i \leq r$*

$$\#\{j \in [n] \mid Fv_j = A_i \text{ and } Cv_j = B_i\} \geq \delta n/|H|^2,$$

and after the projection to the Sylow p-subgroup H_p of H, the elements $A_1, \ldots, A_r$ generate H_p.

Proof. We find the A_i and B_i by induction, so that (after the projection to H_p) the elements $A_1, \ldots, A_k$ generate a p-subgroup of type $\lambda_1, \ldots, \lambda_k$ that is a summand of H_p. Suppose we are done for $i \leq k$. First, we count for how many i is Fv_i order $p^{\lambda_{k+1}}$ in $H_p/\langle A_1, \ldots, A_k\rangle$. Suppose, for the sake of contradiction, that there were fewer than δn. Then we have a $\sigma \subset [n]$ with $|\sigma| < \delta n$ such that $FV_\sigma \neq H$, contradicting the fact that F is a code. So, we have at least δn values of i such that Fv_i is order $p^{\lambda_{k+1}}$ in the projection of $H/\langle A_1, \ldots, A_k\rangle$ to the Sylow p-subgroup of H. There are at most $|H|^2$ possible values for (Fv_i, Cv_i), so we let (A_{k+1}, B_{k+1}) be the most commonly occurring value for at least the δn values of i we have found above. Any element of order $p^{\lambda_{k+1}}$ in an abelian p-group of exponent $p^{\lambda_{k+1}}$ generates a summand. Since after projection to H_p, we have that $\langle A_1, \ldots, A_k\rangle$ is a summand of H_p, and A_{k+1} generates a summand of the quotient $H_p/\langle A_1, \ldots, A_k\rangle$, we see that $\langle A_1, \ldots, A_k, A_{k+1}\rangle$ is as desired. □

Now we will see that robustness does in fact determine that many of our coefficients of interest are non-zero.

Lemma 3.5 (Quadratically many non-zero coefficients for robust C)**.** *Let P be the set of primes dividing the order of G. If $F \in \mathrm{Hom}(V, G)$ is a code of distance δn, and if $C \in \mathrm{Hom}(V, G^*)$ is robust for F, then there are at least $\gamma\delta n^2/(2|G|^2|P|)$ pairs (i, j) with $i \leq j$ such that*

$$E(C, F, i, j) \neq 0.$$

Proof. For each $p \in P$, let G_p be the Sylow p-subgroup of G. Now using $p \in P$ and $F \in \mathrm{Hom}(V, G)$ and $C \in \mathrm{Hom}(V, G^*)$, we pick $A_i(p)$ and $B_i(p)$ as in Lemma 3.4, and let

$$\tau_i(p) := \{j \in [n] \mid Fv_j = A_i \text{ and } Cv_j = B_i\}.$$

Let $\tau(p) := \cup_i \tau_i(p)$. Let V_p be the submodule of V generated by the v_j for $j \in \tau(p)$. In particular, note that FV_p, in the projection to G_p, is all of G_p.

Now, let W be the submodule of V generated by the V_p for all $p \in P$. In particular, note that $FW = G$. So if C is robust for F, by Corollary 3.3,

$$\#\{i \in [n] \mid t(\phi_{C,F}(W), \phi_{F,C}(v_i)) \neq 0\} \geq \gamma n.$$

We have

$$\sum_{p \in P} \#\{i \in [n] \mid t(\phi_{C,F}(V_p), \phi_{F,C}(v_i)) \neq 0\} \geq \#\{i \in [n] \mid t(\phi_{C,F}(W), \phi_{F,C}(v_i)) \neq 0\}$$

because if v_i pairs non-trivially with W, it must pair non-trivial with one of the submodules generating W. So for some $p \in P$, we have

$$\#\{i \in [n] \mid t(\phi_{C,F}(V_p), \phi_{F,C}(v_i)) \neq 0\} \geq \gamma n/|P|.$$

Then for that particular p,

$$\#\{i \in [n] \mid t(\phi_{C,F}(v_j), \phi_{F,C}(v_i)) \neq 0 \text{ for some } j \in \tau(p)\} \geq \gamma n/|P|.$$

However, there are at least $\delta n/|G|^2$ values of $j' \in \tau(p)$ with $\phi_{C,F}(v_{j'}) = \phi_{C,F}(v_j)$. Since for $i < j$ we have $t(\phi_{C,F}(v_j), \phi_{F,C}(v_i)) = E(C, F, i, j)$, and also $t(\phi_{C,F}(v_i), \phi_{F,C}(v_i)) = 2E(C, F, i, i)$, we conclude that there are at least $\gamma\delta n^2/(2|G|^2|P|)$ pairs (i, j) with $i \leq j$ such that $E(C, F, i, j) \neq 0$. □

Next, we will study how many coefficients can be non-zero for weak C. Of course, for $C = 0$, all the $E(C, F, i, j)$ are 0. However, given F, there are other C for which this can happen, and next we will identify those C.

We now take a second equivariant point of view on $E(C, F, i, j)$. There is a natural map coming from the evaluation map $G \otimes G^* \to R$,

$$\mathrm{Hom}(V, G) \otimes \mathrm{Hom}(V, G^*) \to V^* \otimes V^*.$$

We can further compose with the quotient $V^* \otimes V^* \to \mathrm{Sym}^2 V^*$ to obtain

$$\mathrm{Hom}(V, G) \otimes \mathrm{Hom}(V, G^*) \to V^* \otimes V^* \to \mathrm{Sym}^2 V^*.$$

So given an $F \in \mathrm{Hom}(V, G)$, we have a map

(4)

$$m_F : \mathrm{Hom}(V, G^*) \to \mathrm{Sym}^2 V^*,$$
$$C \mapsto \sum_{i=1}^{n} \sum_{j=i+1}^{n} (e(C(v_j), F(v_i)) + e(C(v_i), F(v_j)))v_i^* v_j^* + \sum_{i=1}^{n} e(C(v_i), F(v_i))(v_i^*)^2.$$

First, we determine some elements $C \in \mathrm{Hom}(V, G^*)$ that are in the kernel of m_F; i.e., all the $E(C, F, i, j)$ are 0. For $F \in \mathrm{Hom}(V, G)$ and $u \in G^*$, we can compose F with u to obtain $u(F) \in \mathrm{Hom}(V, R)$. We can then multiply by $v \in G^*$ to obtain $u(F)v \in \mathrm{Hom}(V, G^*)$. So we have a map

$$s_F : \wedge^2 G^* \to \mathrm{Hom}(V, G^*),$$
$$u \wedge v \mapsto u(F)v - v(F)u.$$

We can check that $\mathrm{im}(s_F) \subset \ker(m_F)$ by choosing a generating set for G^*. Let $G \simeq \oplus_{i=1}^{m} \mathbb{Z}/a_i\mathbb{Z}$, with $a_m \mid a_{m-1} \mid \cdots \mid a_1$. Let G^* be given by generators e_i^* and

relations $\frac{a}{a_i}e_i^* = 0$. So using Equation (4), we will check that $\mathrm{im}(s_F) \subset \ker(m_F)$. Let $C = s_F(e_i^* \wedge e_j^*)$. Then the $v_a^* v_b^*$ coefficient of $m_F(C)$ is

$$\begin{aligned}
&e(C(v_b), F(v_a)) + e(C(v_a), F(v_b)) \\
&= e(e_i^*(Fv_b)e_j^* - e_j^*(Fv_b)e_i^*, F(v_a)) + e(e_i^*(Fv_a)e_j^* - e_j^*(Fv_a)e_i^*, F(v_b)) \\
&= e_i^*(Fv_b)e_j^*(Fv_a) - e_j^*(Fv_b)e_i^*(Fv_a) + e_i^*(Fv_a)e_j^*(Fv_b) - e_j^*(Fv_a)e_i^*(Fv_b) \\
&= 0.
\end{aligned}$$

Similarly, the coefficient of $(v_a^*)^2$ in $m_F(s_F(e_i^* \wedge e_j^*))$ is 0. So we conclude $\mathrm{im}(s_F) \subset \ker(m_F)$. (Later, in Lemma 3.7, we will show that $\mathrm{im}(s_F) = \ker(m_F)$ when F is surjective.) We call the C in $\mathrm{im}(s_F)$ *special* for F.

Now we see how many special C there are.

Lemma 3.6. *If $FV = G$, then we have that s_F is injective. In particular, $\# \wedge^2 G | \# \ker(m_F)$.*

Proof. It suffices to show that $\# \wedge^2 G | \# \mathrm{im}(s_F)$. Since everything in sight can be written as a direct sum of Sylow p-subgroups, we can reduce to the case that G is a p-group of type λ (and accordingly assume $R = Z/p^e\mathbb{Z}$). Let $r = \lambda_1'$.

By Lemma 3.4, we can find $\tau \subset [n]$ with $|\tau| = r$ such that Fv_i generate G for $i \in \tau$. Let W be the submodule of V generated by the v_i for $v \in \tau$. Let e_i generate G with relations $p^{\lambda_i} e_i = 0$. Let $w_j \in W$ be such that $Fw_j = e_j$. Let $W' \subset W$ be the subgroup of W generated by the w_j. Note that we have the maps

$$W'/pW' \to W/pW \xrightarrow{F} G/pG.$$

Since W'/pW', W/pW, and G/pG are vector spaces over $\mathbb{F}_p$, with rank at most r, exactly r, and exactly r, respectively, and the composite map above is surjective, we must have that $W'/pW' \to W/pW$ is surjective and thus by Nakayama's Lemma that $W' = W$. Since the r elements $w_1, \ldots, w_r$, generate the free rank r R-module W, they must be a basis, and we have a dual basis w_i^* of W^*.

Let G^* be generated by $e_1^*, \ldots, e_r^*$ with relations $p^{\lambda_i} e_i^* = 0$, and such that $e_i^* e_i = p^{e-\lambda_i}$, and for $i \neq j$ we have $e_i^* e_j = 0$.

Recall we have

$$s_F : \wedge^2 G^* \to \mathrm{Hom}(V, G^*).$$

We can take the further quotient

$$s_F' : \wedge^2 G^* \to \mathrm{Hom}(W, G^*).$$

We see that by the definition of s_F

$$s_F(e_i^* \wedge e_j^*)(w_a) = e_i^*(e_a)e_j^* - e_j^*(e_a)e_i^*.$$

Recall that since W is a free R-module, the natural map $W^* \otimes G^* \to \mathrm{Hom}(W, G^*)$ is an isomorphism. By checking the values on each w_a, we can confirm that

$$s_F'(e_i^* \wedge e_j^*) = p^{e-\lambda_i} w_i^* \otimes e_j^* - p^{e-\lambda_j} w_j^* \otimes e_i^*.$$

For $i < j$, this element has order p^{λ_j}, and we can easily conclude that

$$p^{\lambda_2 + 2\lambda_3 + \cdots + (r-1)\lambda_r} \mid \# \mathrm{im}(s_F') \mid \# \mathrm{im}(s_F). \qquad \square$$

Now we will see that as long as C is not special (in particular even if it is weak), we can get a moderately good bound on the number of non-zero $E(C, F, i, j)$.

Lemma 3.7 (Linearly many non-zero coefficients for non-special C)**.** *Given $F \in \mathrm{Hom}(V,G)$ a code of distance δn, suppose $C \in \mathrm{Hom}(V,G^*) \setminus \mathrm{im}(s_F)$ (so C is not special for F). Then there are at least $\delta n/2$ pairs (i,j) with $i,j \in [n]$ and $i \leq j$ such that*

$$E(C,F,i,j) \neq 0.$$

In other words, not only do we have $\mathrm{im}(s_F) = \ker(m_F)$, but in fact when F is a code, we have that non-special C are not even near $\ker(m_F)$.

Proof. Suppose not, for contradiction. Then let $\pi = \{(i,j) | i,j \in [n]; i \leq j; E(C,F,i,j) \neq 0\}$ and $|\pi| < \delta n/2$. Let σ be the set of all i and j that appear in an $(i,j) \in \pi$. Then $|\sigma| < \delta n$ and for (i,j) with $i \notin \sigma$ or with $j \notin \sigma$ we have $E(C,F,i,j) = 0$.

In Lemma 3.6 we have a lower bound on the size of $\ker(m_F)$. Next we will find a lower bound on the size of $\mathrm{im}(m_F)$. Recall we have

$$m_F : \mathrm{Hom}(V,G^*) \to \mathrm{Sym}^2 V^*,$$
$$C \mapsto \sum_{i=1}^{n} \sum_{j=i+1}^{n} (e(C(v_j),F(v_i)) + e(C(v_i),F(v_j)))v_i^* v_j^* + \sum_{i=1}^{n} e(C(v_i),F(v_i))(v_i^*)^2.$$

We can take the further quotient using $\mathrm{Sym}^2 V^* \to Z$ that sends $v_i^* v_j^*$ to 0 if $i,j \in \sigma$. Call this map

$$m'_F : \mathrm{Hom}(V,G^*) \to Z.$$

So we have some C which is not in $\mathrm{im}(s_F)$ but for which $m'_F(C) = 0$. We will show[6] this is impossible by showing that $(\#G^n/\#\wedge^2 G) | \#\,\mathrm{im}(m'_F)$. Once we have established $(\#G^n/\#\wedge^2 G) \mid \#\,\mathrm{im}(m'_F)$, by combining with Lemma 3.6, we will see that $\mathrm{im}(s_f) = \ker(m'_F)$ and obtain a contradiction, proving the lemma.

As in the proof of Lemma 3.6, we can establish that $(\#G^n/\#\wedge^2 G) | \#\,\mathrm{im}(m'_F)$ by reducing to the case where G is a p-group of type λ, which we will do for the rest of the proof of this lemma (and accordingly assume $R = \mathbb{Z}/p^e\mathbb{Z}$).

We can find $\tau \subset [n] \setminus \sigma$ such that $|\tau| = r$ and Fv_i for $i \in \tau$ generate G using Lemma 3.4. (Specifically, since $|\sigma| < \delta n$, and F is a code of distance δn, we have $FV_\sigma = G$ and so $F|_{V_\sigma}$ is a code of some positive distance. We apply Lemma 3.4 to $F|_{V_\sigma}$.) Let e_i be generators for G with relations $p^{\lambda_i} e_i = 0$. Let G^* be generated by $e_1^*, \ldots, e_r^*$ with relations $p^{\lambda_i} e_i^* = 0$, and such that $e_i^* e_i = p^{e-\lambda_i}$ and for $i \neq j$, we have $e_i^* e_j = 0$. As in the proof of Lemma 3.6, we can find an alternate basis $w_1, \ldots, w_r$ for the free R-module generated by the v_i with $i \in \tau$, with the property that $Fw_i = e_i$.

[6]Our argument below is analogous to the following procedure for finding a lower bound on the rank of a matrix. (1) Cross off some rows (analogous to our consideration of m'_F and m''_F). (2) Find r_1 columns whose remaining (not crossed off) entries have a single non-zero entry and the rest 0, and all those r_1 non-zero entries are in different rows. (The analog of this is done in Equation (5), where the $z_\ell^* \otimes e_m^*$ for $\ell \notin \tau$ and $1 \leq m \leq r$ correspond to the "columns" and the $w_m^* \otimes z_\ell^*$ correspond to the "rows.") (3) Cross off the r_1 rows that have a non-zero entry in one of the columns found in step 2 (analogous to our consideration of m'''_F). (4) Find r_2 columns whose remaining (not crossed off) entries have a single non-zero entry and the rest 0, and all those r_2 non-zero entries are in different rows. (The analog of this is done in Equation (6), where the $z_\ell^* \otimes e_m^*$ for $\ell \in \tau$ and $1 \leq m \leq r$ correspond to the "columns" and the $w_m^* \otimes z_\ell^*$ correspond to the "rows.") (5) Conclude the matrix has rank at least $r_1 + r_2$.

We will in fact consider the further quotient by $\operatorname{Sym}^2 V^* \to Z'$ that sends $v_i^* v_j^*$ to 0 for i, j with neither i nor j in τ. Call this map

$$m_F'' : \operatorname{Hom}(V, G^*) \to Z'.$$

It will now be convenient to pick a new basis, other than the v_i, for V. We do this by replacing v_i (for $i \in \tau$) with the w_k (for $1 \le k \le r$) chosen above. Precisely, for $i \notin \tau$, let $z_i := v_i$. Let $\tau = \{\tau_1, \dots, \tau_r\}$, and for $1 \le i \le r$, let $z_{\tau_i} := w_i$. These z_i are a basis for V, and the corresponding dual basis of V^* we call z_i^*. So $z_i^*(z_j) = 1$ if $i = j$ and is 0 otherwise. (Note that for $i \notin \tau$, we have $z_i^* = v_i^*$.)

If we write $F = \sum_{1 \le i \le n, 1 \le j \le r} f_{ij} z_i^* \otimes e_j$, for any z_ℓ we have

$$F z_\ell = \sum_{1 \le k \le r} f_{\ell k} e_k.$$

Then

$$\begin{aligned} m_F(C) &= \sum_{i=1}^{n} \sum_{j=1, j \ne i}^{n} e(C(z_j), F(z_i)) z_i^* z_j^* + \sum_{i=1}^{n} e(C(z_i), F(z_i))(z_i^*)^2 \\ &= \sum_{i=1}^{n} \sum_{j=1, j \ne i}^{n} e(C(z_j), \sum_{1 \le k \le r} f_{ik} e_k) z_i^* z_j^* + \sum_{i=1}^{n} e(C(z_i), \sum_{1 \le k \le r} f_{ik} e_k)(z_i^*)^2. \end{aligned}$$

So

$$\begin{aligned} &m_F(z_\ell^* \otimes e_m^*) \\ &= \sum_{i=1}^{n} \sum_{j=1, j \ne i}^{n} e(z_\ell^*(z_j) \otimes e_m^*, \sum_{1 \le k \le r} f_{ik} e_k) z_i^* z_j^* + \sum_{i=1}^{n} e(z_\ell^*(z_i) \otimes e_m^*, \sum_{1 \le k \le r} f_{ik} e_k)(z_i^*)^2 \\ &= \sum_{i=1}^{n} \sum_{j=1, j \ne i}^{n} f_{im} p^{e - \lambda_m} z_\ell^*(z_j)(z_i^* z_j^*) + \sum_{i=1}^{n} f_{im} p^{e - \lambda_m} z_\ell^*(z_i)(z_i^*)^2 \\ &= \sum_{i=1}^{n} f_{im} p^{e - \lambda_m} z_i^* z_\ell^*. \end{aligned}$$

Since, $F z_b = \sum_{1 \le k \le r} f_{bk} e_k$, and $F z_{\tau_i} = e_i$, we have $f_{\tau_i i} = 1$ and $f_{\tau_i k} = 0$ for $k \ne i$. If $\ell \notin \tau$,

$$m_F''(z_\ell^* \otimes e_m^*) = \sum_{i \in \tau} f_{im} p^{e - \lambda_m} z_i^* z_\ell^* = \sum_{1 \le i \le r} f_{\tau_i m} p^{e - \lambda_m} w_i^* z_\ell^* = p^{e - \lambda_m} w_m^* z_\ell^*. \tag{5}$$

We see here that $\operatorname{im}(m_F'')$ has a subgroup of size $\#G^{n-r}$. We can then form m_F''', a further quotient to only terms $z_i^* z_j^*$ with $i, j \in \tau$. In particular, the subgroup of size $\#G^{n-r}$ we have identified above will go to 0 under m_F'''. If $\ell \in \tau$,

$$m_F'''(z_\ell^* \otimes e_m^*) = \sum_{i \in \tau} f_{im} p^{e - \lambda_m} z_i^* z_\ell^* = \sum_{1 \le i \le r} f_{\tau_i m} p^{e - \lambda_m} w_i^* z_\ell^* = p^{e - \lambda_m} w_m^* z_\ell^*. \tag{6}$$

So for $i \le j$, we see that $p^{e - \lambda_i} w_i^* w_j^* \in \operatorname{im}(m_F''')$. It follows that $\operatorname{im}(m_F''')$ has a subgroup of size $p^{\lambda_1 r + \cdots + \lambda_r}$. We conclude that $\#G^n / \# \wedge^2 G = \#G^{n-r} p^{\lambda_1 r + \cdots + \lambda_r} \mid \operatorname{im}(m_F'') \mid \operatorname{im}(m_F')$. This completes the proof of the lemma as explained above. □

4. Obtaining the moments II: A good bound for surjections that are codes

In this section, we put the results of the last section together to prove a good bound on the probability that a code descends to a map from the cokernel of a random matrix. If X is a random matrix with integer entries X_{ij}, we say X is *not α-concentrated mod a* if for any prime $p|a$ and any $t \in \mathbb{Z}/p\mathbb{Z}$, the probability $\mathbb{P}(X_{ij} \equiv t \pmod p) \leq 1-\alpha$.

Lemma 4.1. *Let $0 < \alpha < 1$, $\delta > 0$, a is a positive integer, and G is a finite abelian group of exponent dividing a. Then there is a $c > 0$ and a real number K such that the following holds.*

Let X be a random symmetric $n \times n$ matrix, not α-concentrated mod a, whose entries $X_{ij} \in \mathbb{Z}/a\mathbb{Z}$, for $i \leq j$, are independent. Let $F \in \mathrm{Hom}(V, G)$ be a code of distance δn. Let $A \in \mathrm{Hom}(V^*, G)$. For all n we have

$$\left|\mathbb{P}(FX = 0) - |\wedge^2 G||G|^{-n}\right| \leq \frac{K\exp(-cn)}{|G|^n}$$

and

$$\mathbb{P}(FX = A) \leq K|G|^{-n}.$$

From the point of view of descending a surjection to the cokernel of a matrix, we only need $A = 0$ above, but, in fact, for our work with non-codes we will need the case of general A as above. For the proof of Lemma 4.1, we will need the following result.

Lemma 4.2. *Let $\xi \neq 1$ be a bth root of unity, and z a random variable valued in $\mathbb{Z}/b\mathbb{Z}$ that takes each value with probability at most $1-\alpha$. Then $|\mathbb{E}(\xi^z)| \leq \exp(-\alpha/b^2)$.*

Proof. For $t \in \mathbb{Z}/b\mathbb{Z}$, let $p_t = \mathbb{P}(z = t)$. We have $0 \leq p_t \leq 1-\alpha$ with $\sum_t p_t = 1$. Then we will see $|\sum_t p_t\xi^t| \leq e^{-\alpha/b^2}$. Let U be a unit vector in the same direction as $E := \sum_t p_t\xi^t$ in the complex plane. We consider the projections of the ξ^t onto U and their (signed) lengths $proj_U(\xi^t)$. We have $E = U\sum_t p_t proj_U(\xi^t)$. Let $c \in \mathbb{Z}/b\mathbb{Z}$ be so that among the ξ^t, the complex number ξ^c is closest to U in angle. So for $t \neq c$, we have $proj_U(\xi^t) \leq \cos(\pi/b)$. So

$$\sum_t p_t proj_U(\xi^t) \leq \cos(\pi/b) + p_c(1-\cos(\pi/b)) \leq \alpha\cos(\pi/b) + 1 - \alpha.$$

We have $-1 + \cos(\pi/b) \leq -b^{-2}$ for $b \geq 1$. So $-1 + \cos(\pi/b) \leq -b^{-2}e^{-\alpha/b^2}$. Integrating with respect to α, we obtain $\alpha\cos(\pi/b) + 1 - \alpha \leq e^{-\alpha/b^2}$, and conclude $|\sum_t p_t\xi^t| \leq e^{-\alpha/b^2}$, as desired. □

Now we are ready to prove Lemma 4.1.

Proof of Lemma 4.1. Recall,

$$\mathbb{P}(FX = A) = \frac{1}{|G|^n}\sum_{C \in \mathrm{Hom}(V,G^*)} \mathbb{E}(\zeta^{C(FX-A)}),$$

where ζ is a primitive ath root of unity.

We break the sum into 3 pieces: (we will later choose $0 < \gamma < \delta$)

(1) when C is special for F,
(2) when C is not special for F and is weak for F,
(3) when C is robust for F.

Given F, there are $|\wedge^2 G|$ special C for which $\zeta^{C(FX)} = 1$ for all X. Thus, the sum from (1) contributes $|\wedge^2 G||G|^{-n}$ when $A = 0$ and at most $|\wedge^2 G||G|^{-n}$ in absolute value for any A.

For (2), we will first use the fact that there are not too many weak C and our bound from Lemma 3.7. From Lemma 3.1, we have that the number of $C \in \mathrm{Hom}(V, G^*)$ such that C is weak for F is at most

$$C_G \binom{n}{\lceil \gamma n \rceil - 1} |G|^{\gamma n}.$$

Next we factor the expected value

$$\mathbb{E}(\zeta^{C(FX-A)}) = \mathbb{E}(\zeta^{C(-A)}) \prod_{1 \le i < j \le n} \mathbb{E}(\zeta^{E(C,F,i,j)X_{ij}}) \prod_{1 \le i \le n} \mathbb{E}(\zeta^{E(C,F,i,i)X_{ii}}).$$

Let $u \in R = \mathbb{Z}/a\mathbb{Z}$ with $u \neq 0$. So by Lemma 4.2, we have $|\mathbb{E}(\zeta^{uX_{ij}})| \le \exp(-\alpha/a^2)$.

Given F a code of distance δn and a C that is not special, by Lemma 3.7 we have that at least $\delta n/2$ of the $E(F, C, i, j)$ are non-zero. So if C is not special for F, we conclude that

$$|\mathbb{E}(\zeta^{C(FX-A)})| \le \exp(-\alpha\delta n/(2a^2)).$$

Now, given F and a robust C for F, by Lemma 3.5, we have that at least $\gamma\delta n^2/(2|G|^2|P|)$ of the $E(C, F, i, j)$ are non-zero (where P is the set of primes dividing a). So if C is robust for F, we conclude that

$$|\mathbb{E}(\zeta^{C(FX-A)})| \le \exp(-\alpha\gamma\delta n^2/(2|G|^2|P|a^2)).$$

In conclusion

$$\left| \mathbb{P}(FX = A) - \frac{1}{|G|^n} \sum_{C \in \mathrm{Hom}(V,G^*),\ \text{special}} |\mathbb{E}(\zeta^{C(FX-A)}) \right|$$
$$\le \frac{1}{|G|^n} \sum_{C \in \mathrm{Hom}(V,G^*),\ \text{not special}} |\mathbb{E}(\zeta^{C(FX-A)})|$$
$$\le \frac{1}{|G|^n} \left(C_G \binom{n}{\lceil \gamma n \rceil - 1} |G|^{\gamma n} \exp(-\alpha\delta n/(2a^2)) + |G|^n \exp(-\alpha\gamma\delta n^2/(2|G|^2|P|a^2)) \right).$$

So for any $c > 0$ such that $c < \alpha\delta/(2a^2)$, given δ, α, G, c, we can choose γ sufficiently small so that we have

$$\left| \mathbb{P}(FX = A) - \frac{1}{|G|^n} \sum_{C \in \mathrm{Hom}(V,G^*),\ \text{special}} \mathbb{E}(\zeta^{C(FX-A)}) \right|$$
$$\le \frac{1}{|G|^n} \left(C_G \exp(-cn) + \exp(\log(|G|)n - \alpha\gamma\delta n^2/(2|G|^2|P|a^2)) \right).$$

For n sufficiently large given $\alpha, G, \delta, c, \gamma$, we have

$$\log(|G|)n - \alpha\gamma\delta n^2/(2|G|^2|P|a^2) \le -cn.$$

So in the case $A = 0$, for n sufficiently large, we have

$$\left|\mathbb{P}(FX = 0) - |\wedge^2 G||G|^{-n}\right| \leq \frac{(C_G + 1)\exp(-cn)}{|G|^n}.$$

For n that are not sufficiently large, we will just increase the constant K in the lemma.

For any A, we have for n sufficiently large given $\alpha, |G|, \delta, c, \gamma$,

$$\begin{aligned}\mathbb{P}(FX = A) &\leq \left|\frac{1}{|G|^n}\sum_{C\in \mathrm{Hom}(V,G^*),\ \mathrm{special}} \mathbb{E}(\zeta^{C(FX-A)})\right| + \frac{(C_G+1)\exp(-cn)}{|G|^n}\\ &\leq |G|^{-n}(|\wedge^2 G| + C_G + 1).\end{aligned}$$

For n that are not sufficiently large, we can increase the constant K as necessary. □

5. Obtaining the moments III: Determining the structural properties of the surjections

In the last section, we dealt with $F \in \mathrm{Hom}(V, G)$ that were codes. Unfortunately, it is not sufficient to divide F into codes and non-codes. We need a more delicate division of F based on the subgroups of G. For an integer D with prime factorization $\prod_i p_i^{e_i}$, let $\ell(D) = \sum_i e_i$.

Definition. The *depth* of an $F \in \mathrm{Hom}(V, G)$ is the maximal positive D such that there is a $\sigma \subset [n]$ with $|\sigma| < \ell(D)\delta n$ such that $D = [G : FV_\sigma]$, or is 1 if there is no such D. (When using this definition, we will always assume $\delta < \ell(|G|)^{-1}$.)

Remark 5.1. In particular, if the depth of F is 1, then for every $\sigma \subset [n]$ with $|\sigma| < \delta n$, we have that $FV_\sigma = G$ (as otherwise $\ell([G : FV_\sigma]) \geq 1$), and so we see that F is a code of distance δn. We have handled F that are codes in the previous section, and for each larger depth, we compare F to a combination of a depth 1 "F" for the subgroup FV_σ of G (and an "F" for the quotient group G/FV_σ of G (where we use an Odlyzko-type bound).

Also, if the depth of F is D, then $D \mid \#G$. Now we will bound the number of F that we have of depth D.

Lemma 5.2 (Count F of given depth)**.** *There is a constant K depending on G such that if $D > 1$, then number of $F \in \mathrm{Hom}(V, G)$ of depth D is at most*

$$K\binom{n}{\lceil \ell(D)\delta n\rceil - 1}|G|^n|D|^{-n+\ell(D)\delta n}.$$

Proof. We sum over $\sigma \subset [n]$ with $|\sigma| = \lceil \ell(D)\delta n\rceil - 1$ the number of F such that $D = [G : FV_\sigma]$. Then we sum over the subgroups of G of index D (this sum will go into the constant). Now given a particular subgroup H of index D, we bound the number of F such that $FV_\sigma = H$. We have at most $(|G|/D)^{(n-|\sigma|)}$ maps from V_σ to H, and at most $|G|^{|\sigma|}$ choices for the Fv_i with $i \in \sigma$. So, for a particular σ and H, the number of F such that $FV_\sigma = H$ is at most

$$(|G|/D)^{(n-|\sigma|)}|G|^{|\sigma|} = |G|^n D^{-n+|\sigma|}.$$

Note that $|\sigma| < \ell(D)\delta n$, and the lemma follows. □

The following is a variant on the bound on the number of F of depth D that we will need when we are working with the Laplacian of a random graph. Note that if G is a finite abelian group of exponent dividing a, then so is $G \oplus R$, and so we can apply the definition of depth above to an $F \in \mathrm{Hom}(V, G \oplus R)$ (where G in the definition would be replaced with $G \oplus R$).

Lemma 5.3. *Let $pr_2 : G \oplus R \to R$ be the projection onto the second factor. There is a constant K depending on G such that if $D > 1$, then the number of $F \in \mathrm{Hom}(V, G \oplus R)$ such that $pr_2(Fv_i) = 1$ for all $i \in [n]$ and of depth D is at most*

$$K \binom{n}{\lceil \ell(D)\delta n \rceil - 1} |G|^n |D|^{-n+\ell(D)\delta n}.$$

Proof. Let $G' = G \oplus R$. Note that $|G'| = a|G|$. We sum over $\sigma \subset [n]$ with $|\sigma| = \lceil \ell(D)\delta n \rceil - 1$ the number of F such that FV_σ has index D in G'. Then we sum over the subgroups of G' of index D (this sum will go into the constant). Now given a particular subgroup H of index D, we bound the number of F such that $FV_\sigma = H$.

For $i \in [n] \setminus \sigma$, we must have $Fv_i \in H$ and $pr_2(Fv_i) = 1$. There are at most $|H|/a$ elements $h \in H$ such that $pr_2(h) = 1$. So there are at most

$$(|H|/a)^{n-|\sigma|} = (|G'|/(aD))^{n-|\sigma|} = (|G|/D)^{n-|\sigma|}$$

possibilities for $F|_{V_\sigma}$. There are at most $|G|^{|\sigma|}$ choices for the Fv_i with $i \in \sigma$. So, for a particular σ and H, the number of F such that $FV_\sigma = H$ (and $pr_2(Fv_i) = 1$ for all $i \in [n]$) is at most

$$(|G|/D)^{n-|\sigma|} |G|^{|\sigma|} = |G|^n D^{-n+|\sigma|}.$$

Note that $|\sigma| < \ell(D)\delta n$, and the lemma follows. □

For each depth D of F, we will use the following specially tailored bound for $\mathbb{P}(FX = 0)$.

Lemma 5.4 (Bound probability given depth)**.** *Let α, δ, G, a be as in Lemma* 4.1. *Then there is a real number K such that if $F \in \mathrm{Hom}(V, G)$ has depth $D > 1$ and $[G : FV] < D$ (e.g., the latter is true of $FV = G$), then for all X as in Lemma* 4.1 *and all n,*

$$\mathbb{P}(FX = 0) \le K e^{-\alpha(1-\ell(D)\delta)n} (|G|/D)^{-(1-\ell(D)\delta)n}.$$

Proof. Pick a $\sigma \subset [n]$ with $|\sigma| < \ell(D)\delta n$ such that $D = [G : FV_\sigma]$. Let $FV_\sigma = H$.

We will now divide the elements $i \in [n]$ depending on whether $Fv_i \in H$. Let η be the set of i such that $Fv_i \in H$. Let $\tau = [n] \setminus \eta$. Note that $[n] \setminus \sigma \subset \eta$, so $\tau \subset \sigma$, and so $|\tau| < \ell(D)\delta n$. However, since $[G : FV] < D$, we cannot have τ empty.

Let X_η be obtained from X by replacing the entries in the τ rows with 0, and let X_τ be obtained from X by replacing the entries in the η rows with 0. Note that $FX \in \mathrm{Hom}(V^*, G)$. We identify $\mathrm{Hom}(V^*, G)$ with G^n using the preferred basis of V^*. We have

$$\mathbb{P}(FX = 0) = \mathbb{P}(FX_\tau \in H^n)\mathbb{P}(FX = 0 | FX_\tau \in H^n).$$

Let $X_{\tau\eta}$ be obtained from X_τ by replacing the entries in the τ columns with 0. We have

$$\mathbb{P}(FX_\tau \in H^n) \le \mathbb{P}(FX_{\tau\eta} \in H^n).$$

Note that all the entries in $X_{\tau\eta}$ that we have not made zero are independent. So if $\mathrm{col}_i(X_\tau)$ denotes the ith column of X_τ,

$$\mathbb{P}(FX_{\tau\eta} \in H^n) = \prod_{i\in\eta} \mathbb{P}(F\,\mathrm{col}_i(X_\tau) \in H).$$

Consider a single column and let $x_1, \dots, x_{|\tau|}$ be the entries in the τ rows of X, and $f_1, \dots, f_{|\tau|} \in G \setminus H$ be the corresponding entries of F. We condition on $x_2, \dots, x_{|\tau|}$. Then, for some fixed $g \in G$, and $f_1 \in G \setminus H$, we are trying to bound

$$\mathbb{P}(f_1 x_1 \equiv g \text{ in } G/H).$$

Since $f_1 \not\equiv 0 \pmod{G/H}$, there is some prime p that divides the order of f_1 in G/H. Note that if $f_1 x \equiv g$ in G/H, then for $\Delta \in \mathbb{Z}$ such that $p \nmid \Delta$, we have $f_1(x+\Delta) \not\equiv g$ in G/H. So the x such that $f_1 x \equiv g$ in G/H are contained in a single equivalence class modulo p. Thus,

$$\mathbb{P}(f_1 x_1 \equiv a \text{ in } G/H) \le e^{-\alpha},$$

since the probability that x_1 is any particular equivalence class mod p is at most $e^{-\alpha}$. We can then conclude

$$\mathbb{P}(FX_\tau \in H^n) \le e^{-\alpha|\eta|}.$$

Now let $X_{\eta\eta}$ be obtained from X_η by replacing the entries in τ columns with 0. Let $X_{*\eta} = X_{\eta\eta} + X_{\tau\eta}$ (so $X_{*\eta}$ is obtained from X by replacing the τ columns with 0). We have

$$\mathbb{P}(FX = 0 | FX_\tau \in H^n) \le \mathbb{P}(FX_{*\eta} = 0 | FX_\tau \in H^n).$$

We estimate $\mathbb{P}(FX_{*\eta} = 0 | FX_\tau \in H^n)$ by conditioning on the τ rows (and columns) of X. Then for any $n \times n$ matrix Y_τ over R supported on the τ rows with $FY_\tau \in H^n$ (and with $Y_{\tau\eta}$ obtained from Y_τ by replacing the entries in the τ columns by 0),

$$\mathbb{P}(FX_{*\eta} = 0 | X_\tau = Y_\tau) = \mathbb{P}(FX_{\eta\eta} + FY_{\tau\eta} = 0 | X_\tau = Y_\tau).$$

In particular, $FY_{\tau\eta}$ is some fixed value in $H^{|\eta|}$. Also, note that $X_{\eta\eta}$ is independent of X_τ. For a fixed $A \in H^{|\eta|}$, we need to estimate $\mathbb{P}(FX_{\eta\eta} = A)$. Note that $F|_{V_\tau}$ (i.e., restricted to the η indices) is a code of distance δn in $\mathrm{Hom}(V_\tau, H)$. (If it were not, then by eliminating τ and $< \delta n$ indices, we would eliminate fewer than $(\ell(D)+1)\delta n$ indices and have an image which was an index that D strictly divides, contradicting the depth of F.) So by Lemma 4.1, for some K

$$\mathbb{P}(FX_{\eta\eta} + FY_{\tau\eta} = 0 | X_\tau = Y_\tau) = \mathbb{P}(FX_{\eta\eta} = -FY_{\tau\eta} \in H^{|\eta|}) \le K|H|^{-|\eta|}.$$

So we conclude

$$\mathbb{P}(FX = 0) \le Ke^{-\alpha|\eta|}|H|^{-|\eta|} \le K_1 e^{-\alpha(1-\ell(D)\delta)n}(|G|/D)^{-(1-\ell(D)\delta)n}. \quad \square$$

6. Obtaining the moments IV: Putting it all together

We can combine our work above to give a universality result on (and the actual values of) the moments of cokernels of random matrices and of sandpile groups of random graphs, which we do in the following two theorems, respectively. Recall the definition of α-concentrated from Section 4.

Theorem 6.1. *Let $0 < \alpha < 1$ be a real number and G a finite abelian group. For any c sufficiently small, there is a $K > 0$ (depending on α, G, c) such that the following holds. Let X be a random symmetric $n \times n$ matrix, not α-concentrated mod $|G|$, whose entries $X_{ij} \in \mathbb{Z}$, for $i \le j$, are independent. Then,*

$$\left|\mathbb{E}(\#\operatorname{Sur}(\operatorname{cok}(X), G)) - |\wedge^2 G|\right| \le Ke^{-cn}.$$

Proof. We omit the details in this proof, as they are almost identical to (and slightly simpler than) the details in the proof of our next result, Theorem 6.2, which is in the case of main interest. If the exponent of G divides a, we can reduce X modulo a so as to agree with our notation above. We wish to estimate $\sum_{F\in\operatorname{Sur}(V,G)} \mathbb{P}(FX = 0)$. Using Lemmas 5.2 and 5.4 we have

$$\sum_{\substack{F\in\operatorname{Sur}(V,G)\\ F \text{ not code of distance } \delta n}} \mathbb{P}(FX = 0) \le Ke^{-cn}.$$

Also, from Lemma 5.2

$$\sum_{\substack{F\in\operatorname{Sur}(V,G)\\ F \text{ not code of distance } \delta n}} |\wedge^2 G||G|^{-n} \le Ke^{-cn}.$$

We also have

$$\sum_{F\in\operatorname{Hom}(V,G)\setminus\operatorname{Sur}(V,G)} |\wedge^2 G||G|^{-n} \le K2^{-n}.$$

Then we have, using Lemma 4.1,

$$\sum_{\substack{F\in\operatorname{Sur}(V,G)\\ F \text{ code of distance } \delta n}} \left|\mathbb{P}(FX = 0) - |\wedge^2 G||G|^{-n}\right| \le Ke^{-cn}.$$

Combining, we obtain the theorem. □

In particular, the following theorem implies Theorem 1.2.

Theorem 6.2. *Let $0 < q < 1$, and let G be a finite abelian group. Then there exist $c, K > 0$ (depending on G) such that if $\Gamma \in G(n, q)$ is a random graph, S is its sandpile group, and for all n we have*

$$\left|\mathbb{E}(\#\operatorname{Sur}(S, G)) - |\wedge^2 G|\right| \le Ke^{-cn}.$$

Proof. Let a be the exponent of G. Let $R = \mathbb{Z}/a\mathbb{Z}$. Note that $\#\operatorname{Sur}(S, G) = \#\operatorname{Sur}(S \otimes R, G)$, so throughout this proof we will let $\bar{S} := S \otimes R$. We let $\bar{L}$ be the reduction of the Laplacian L modulo a, so $\bar{L}$ is an $n \times n$ matrix with coefficients in R.

We let X be an $n \times n$ random symmetric matrix with coefficients in R with X_{ij} distributed as $\bar{L}_{ij}$ for $i < j$ and with X_{ii} distributed uniformly in R, with all X_{ij} (for $i < j$) and X_{ii} independent. Let $F_0 \in \operatorname{Hom}(V, R)$ be the map that sends each v_i to 1. Now, X and $\bar{L}$ do not have the same distribution, as the column sums of X can be anything and the column sums of $\bar{L}$ are zero, i.e., $F_0\bar{L} = 0$. However, if

we condition on $F_0X = 0$, then we find that this conditioned distribution of X is the same as the distribution of $\bar{L}$. Given X and conditioning on the off diagonal entries, we see that the probability that $F_0X = 0$ is a^{-n} (for any choice of off diagonal entries). So any choice of off diagonal entries is equally likely in $\bar{L}$ as in X conditioned on $F_0X = 0$.

Recall $V = R^n$. So for $F \in \mathrm{Hom}(V, G)$, we have

$$\mathbb{P}(F\bar{L} = 0) = \mathbb{P}(FX = 0 | F_0X = 0) = \mathbb{P}(FX = 0 \text{ and } F_0X = 0)a^n.$$

Let $\tilde{F} \in \mathrm{Hom}(V, G \oplus R)$ be the sum of F and F_0.

Let $Z \subset V$ denote the vectors whose coordinates sum to 0, i.e., $Z = \{v \in V \mid F_0v = 0\}$. Let $\mathrm{Sur}^*(V, G)$ denote the maps from V to G that are a surjection when restricted to Z. We wish to estimate

$$\begin{aligned}
\mathbb{E}(\#\,\mathrm{Sur}(\bar{S}, G)) &= \mathbb{E}(\#\,\mathrm{Sur}(Z/\,\mathrm{col}(\bar{L}), G)) \\
&= \sum_{F \in \mathrm{Sur}(Z,G)} \mathbb{P}(F\bar{L} = 0) \\
&= \frac{1}{|G|} \sum_{F \in \mathrm{Sur}^*(V,G)} \mathbb{P}(F\bar{L} = 0) \\
&= |G|^{-1} a^n \sum_{F \in \mathrm{Sur}^*(V,G)} \mathbb{P}(\tilde{F}X = 0).
\end{aligned}$$

Note that if $F : V \to G$ is a surjection when restricted to Z, then $\tilde{F}$ is a surjection from V to $G \oplus R$.

We start by considering the part of the sum to which we can apply Lemma 5.4. We let K change in each line, as long as it is a constant depending only on q, G, δ. Let $\alpha = \max(q, 1 - q)$. We then have

$$\begin{aligned}
&\frac{a^n}{|G|} \sum_{\substack{F \in \mathrm{Sur}^*(V,G) \\ \tilde{F} \text{ not code of distance } \delta n}} \mathbb{P}(\tilde{F}X = 0) \\
&\leq \frac{a^n}{|G|} \sum_{\substack{D > 1 \\ D | \#G}} \sum_{\substack{F \in \mathrm{Sur}^*(V,G) \\ \tilde{F} \text{ depth } D}} \mathbb{P}(\tilde{F}X = 0) \qquad \text{(by Remark 5.1)} \\
&\leq \frac{a^n}{|G|} \sum_{\substack{D > 1 \\ D | \#G}} \#\{\tilde{F} \in \mathrm{Hom}(V, G \oplus R) \text{ depth } D \mid pr_2(v_i) = 1 \text{ for all } i\} \\
&\quad \times Ke^{-\alpha(1-\ell(D)\delta)n}(a|G|/D)^{-(1-\ell(D)\delta)n} \\
&\leq \frac{a^n}{|G|} \sum_{\substack{D > 1 \\ D | \#G}} K \binom{n}{\lceil \ell(D)\delta n \rceil - 1} |G|^n D^{-n+\ell(D)\delta n} \\
&\quad \times e^{-\alpha(1-\ell(D)\delta)n}(a|G|/D)^{-(1-\ell(D)\delta)n} \qquad \text{(by Lemma 5.3)} \\
&\leq K \binom{n}{\lceil \ell(|G|)\delta n \rceil - 1} e^{-\alpha(1-\ell(|G|)\delta)n}(a|G|)^{\delta\ell(|G|)n} \\
&\leq Ke^{-cn}.
\end{aligned}$$

For any $0 < c < \alpha$, we can choose δ small enough so that

$$\binom{n}{\lceil \ell(|G|)\delta n\rceil - 1} e^{-\alpha(1-\ell(|G|)\delta)n}(a|G|)^{\delta\ell(|G|)n} \le e^{-cn},$$

and the last inequality in the long chain above holds.

Also,

$$\begin{aligned}
\sum_{\substack{F\in \mathrm{Sur}^*(V,G)\\ \tilde F \text{ not code of distance } \delta n}} |\wedge^2 G||G|^{-n} &\le \sum_{\substack{D>1\\ D|\#G}} \sum_{\substack{F\in \mathrm{Sur}^*(V,G)\\ \tilde F \text{ depth } D}} |\wedge^2 G||G|^{-n}\\
\text{(by Lemma 5.3)} &\le \sum_{\substack{D>1\\ D|\#G}} K\binom{n}{\lceil \ell(D)\delta n\rceil - 1}|G|^n|D|^{-n+\ell(D)\delta n}|\wedge^2 G||G|^{-n}\\
&\le K\binom{n}{\lceil \ell(|G|)\delta n\rceil - 1}2^{-n+\ell(|G|)\delta n}\\
&\le Ke^{-cn}.
\end{aligned}$$

For any $0<c<\log(2)$, we can choose δ small enough so that $\binom{n}{\lceil \ell(|G|)\delta n\rceil -1}2^{-n+\ell(|G|)\delta n}\le e^{-cn}$, and the last inequality above holds.

We also have

$$\begin{aligned}
\sum_{F\in \mathrm{Hom}(V,G)\setminus \mathrm{Sur}^*(V,G)} |\wedge^2 G||G|^{-n} &\le \sum_{H \text{ proper s.g of } G} \sum_{F\in \mathrm{Hom}(Z,H)} |\wedge^2 G||G|^{-n+1}\\
&\le \sum_{H \text{ proper s.g of } G} |H|^{n-1}|\wedge^2 G||G|^{-n+1}\\
&\le K2^{-n}.
\end{aligned}$$

Then we have, using Lemma 4.1,

$$\begin{aligned}
&\sum_{\substack{F\in \mathrm{Sur}^*(V,G)\\ \tilde F \text{ code of distance } \delta n}} \left|\mathbb{P}(\tilde F X = 0) - |\wedge^2 (G\oplus R)|(a|G|)^{-n}\right|\\
&\le \sum_{\substack{F\in \mathrm{Sur}^*(V,G)\\ \tilde F \text{ code of distance } \delta n}} Ke^{-cn}(a|G|)^{-n}\\
&\le Ke^{-cn}a^{-n}.
\end{aligned}$$

In conclusion

$$\begin{aligned}
&\left|\frac{a^n}{|G|}\left(\sum_{F\in \mathrm{Sur}^*(V,G)} \mathbb{P}(\tilde{F}X=0)\right) - |\wedge^2 G|\right| \\
&\leq \left|\frac{a^n}{|G|} \sum_{\substack{F\in \mathrm{Sur}^*(V,G)\\ \tilde{F} \text{ not code of distance } \delta n}} \mathbb{P}(\tilde{F}X=0)\right| \\
&\quad + \frac{a^n}{|G|} \sum_{\substack{F\in \mathrm{Sur}^*(V,G)\\ \tilde{F} \text{ code of distance } \delta n}} \left|\mathbb{P}(\tilde{F}X=0) - |\wedge^2 (G\oplus R)|(a|G|)^{-n}\right| \\
&\quad + \left|-|\wedge^2 G| + \sum_{\substack{F\in \mathrm{Sur}^*(V,G)\\ \tilde{F} \text{ code of distance } \delta n}} |\wedge^2 (G\oplus R)|(a|G|)^{-n}\right| \\
&\leq Ke^{-cn} + \sum_{\substack{F\in \mathrm{Sur}^*(V,G),\\ \tilde{F} \text{ not code of distance } \delta n}} |\wedge^2 G||G|^{-n} + \sum_{F\in \mathrm{Hom}(V,G)\setminus \mathrm{Sur}^*(V,G)} |\wedge^2 G||G|^{-n} \\
&\leq Ke^{-cn}.
\end{aligned}$$

Recall from above, we have

$$\mathbb{E}(\#\,\mathrm{Sur}(S,G)) = |G|^{-1}a^n \sum_{F\in \mathrm{Sur}^*(V,G)} \mathbb{P}(\tilde{F}X=0),$$

and so we conclude the proof of the theorem. □

7. Basic estimates on abelian groups

In this section we collect some basic estimates on numbers of maps between finite abelian groups. We do not claim any originality of the results in this section, but we merely collect them here for completeness and easy reference.

We write G_λ for the abelian p-group of type λ. The following two lemmas are standard.

Lemma 7.1. *We have*

$$|\,\mathrm{Hom}(G_\mu, G_\lambda)| = p^{\sum_i \mu'_i\lambda'_i}.$$

Proof. Since for finite abelian groups A, B, C, we have $\mathrm{Hom}(A\oplus B, C) \simeq \mathrm{Hom}(A,C)\times \mathrm{Hom}(B,C)$ and $\mathrm{Hom}(A, B\oplus C) \simeq \mathrm{Hom}(A,B)\times \mathrm{Hom}(A,C)$, it suffices to check that the lemma holds for cyclic groups and that the formula respects this multiplicativity, each of which is clear. □

Lemma 7.2 (e.g., Theorem 4.1 of [HR07])**.** *We have*

$$|\,\mathrm{Aut}(G_\lambda)| = p^{\sum_i (\lambda'_i)^2} \prod_{i=1}^{\lambda_1}\prod_{j=1}^{m_i}(1-p^{-j}).$$

The following lemma is used in the Introduction to write down an explicit formula for the probabilities of particular groups.

Lemma 7.3. *If G is a finite abelian p-group of type λ,*

$$\#\{\text{symmetric, bilinear, perfect } \phi : G \times G \to \mathbb{C}^*\}$$
$$= p^{\sum_i \lambda_i'(\lambda_i'+1)/2} \prod_{i=1}^{\lambda_1} \prod_{j=1}^{\lceil \frac{\lambda_i' - \lambda_{i+1}'}{2} \rceil} (1 - p^{1-2j}).$$

Proof. Since any such ϕ has an image in the p^{λ_1}th roots of unity, we replace $\mathbb{C}^*$ by $p^{-\lambda_1}\mathbb{Z}/\mathbb{Z}$, in order to be able to use additive notation. We can write G as an abelian group with generators $e_1, \dots, e_{\lambda_1'}$ and relations $p^{\lambda_j} e_j = 0$. We can write $\operatorname{Hom}(G, p^{-\lambda_1}\mathbb{Z}/\mathbb{Z})$ then with generators $\hat{e}_j$ such that $\hat{e}_j(e_j) = p^{-\lambda_j}$ and $\hat{e}_j(e_k) = 0$ for $k \neq j$.

A symmetric bilinear pairing $G \times G \to p^{-\lambda_1}\mathbb{Z}/\mathbb{Z}$ is the same as a homomorphism $G \to \operatorname{Hom}(G, p^{-\lambda_1}\mathbb{Z}/\mathbb{Z})$, which can be given explicitly as

$$e_j \mapsto \sum_{\substack{k \\ \lambda_k \leq \lambda_j}} (e_j, e_k)\hat{e}_k + \sum_{\substack{k \\ \lambda_k > \lambda_j}} (e_j, e_k) p^{\lambda_k - \lambda_j} \hat{e}_k$$

for any choices of $(e_j, e_k) \in \mathbb{Z}/p^{\min(\lambda_j, \lambda_k)}\mathbb{Z}$ such that $(e_j, e_k) = (e_k, e_j)$. Thus there are $p^{\sum_i \lambda_i'(\lambda_i'+1)/2}$ choices of symmetric bilinear pairings $G \times G \to p^{-\lambda_1}\mathbb{Z}/\mathbb{Z}$.

Now we will compute how many of these are perfect, i.e., induce isomorphisms $G \to \operatorname{Hom}(G, p^{-\lambda_1}\mathbb{Z}/\mathbb{Z})$. By Nakayama's Lemma, a homomorphism $\phi : G \to \operatorname{Hom}(G, p^{-\lambda_1}\mathbb{Z}/\mathbb{Z})$ is an isomorphism if and only if it is an isomorphism modulo p. In $\operatorname{Hom}(G, p^{-\lambda_1}\mathbb{Z}/\mathbb{Z})/p\operatorname{Hom}(G, p^{-\lambda_1}\mathbb{Z}/\mathbb{Z})$, we see that $p^{\lambda_k - \lambda_j}\hat{e}_k$ is trivial if $\lambda_k > \lambda_j$. Thus it follows from the block upper triangular shape of the map $G/pG \to \operatorname{Hom}(G, p^{-\lambda_1}\mathbb{Z}/\mathbb{Z})/p\operatorname{Hom}(G, p^{-\lambda_1}\mathbb{Z}/\mathbb{Z})$ that this map is an isomorphism if and only if for every i, the (e_j, e_k) for elements e_j, e_k among the $\lambda_i' - \lambda_{i+1}'$ generators with order p^i form an invertible matrix mod p. Using the fact that

$$\#\{\text{symmetric matrices in } \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})\} = p^{\frac{n(n+1)}{2}} \prod_{j=1}^{\lceil n/2 \rceil} (1 - p^{1-2j})$$

(e.g., from [Mac69, Theorem 2]), and the fact that in the quotient from homomorphisms $G \to \operatorname{Hom}(G, p^{-\lambda_1}\mathbb{Z}/\mathbb{Z})$ to homomorphisms $G/pG \to \operatorname{Hom}(G, p^{-\lambda_1}\mathbb{Z}/\mathbb{Z})/p\operatorname{Hom}(G, p^{-\lambda_1}\mathbb{Z}/\mathbb{Z})$, all the fibers have the same size, we conclude the lemma. □

Lemma 7.4. *Let μ and λ be partitions. Let $G_{\mu,\lambda}$ be the set of subgroups of G_λ that are isomorphic to G_μ. Then*

$$|G_{\mu,\lambda}| \leq \frac{1}{(\prod_{i \geq 1}(1 - 2^{-i}))^{\lambda_1}} p^{\sum_{i=1}^{\lambda_1} \mu_i'\lambda_i' - (\mu_i')^2}.$$

Proof. It is standard that

$$|G_{\mu,\lambda}| = \prod_{i \geq 1} \left(p^{\mu_i'\lambda_i' - (\mu_i')^2} \left(\prod_{k=1}^{\mu_i' - \mu_{i+1}'} \frac{1 - p^{-\lambda_i' + \mu_i' - k}}{1 - p^{-k}} \right) \right)$$

(see, e.g., [But87, Equation (1)]). Note that for i such that $\lambda_i' = 0$, then if $\mu_i' > 0$, then $|G_{\mu,\lambda}| = 0$, and otherwise the inner product above is 1. Thus

$$\begin{aligned}|G_{\mu,\lambda}| &= p^{\sum_{i=1}^{\lambda_1} \mu_i'\lambda_i' - (\mu_i')^2} \prod_{i=1}^{\lambda_1} \left(\prod_{k=1}^{\mu_i'-\mu_{i+1}'} \frac{1-p^{-\lambda_i'+\mu_i'-k}}{1-p^{-k}} \right) \\ &= p^{\sum_{i=1}^{\lambda_1} \mu_i'\lambda_i' - (\mu_i')^2} \prod_{i=1}^{\lambda_1} \left(\prod_{k=1}^{\infty} \frac{1}{1-p^{-k}} \right).\end{aligned}$$

The lemma follows using $p \geq 2$. (It will be simpler later to have a single bound for all p.) □

Lemma 7.5. *Let G_λ be an abelian p-group of type λ. Let $F = \frac{2}{1-2^{-1/8}} \prod_{i\geq 1} (1-2^{-i})^{-1}$. We have*

$$\sum_{G_1 \text{ subgroup of } G} |\wedge^2 G_1| \leq F^{\lambda_1} p^{\sum_i \frac{\lambda_i'(\lambda_i'-1)}{2}}.$$

Proof. We have

$$\sum_{G_1 \text{ subgroup of } G} |\wedge^2 G_1| = \sum_{\mu} |G_{\mu,\lambda}| p^{\sum_i \frac{\mu_i'(\mu_i'-1)}{2}}.$$

Note that we only have to sum over μ that are subpartitions of λ, or else $|G_{\mu,\lambda}| = 0$. In particular, we only have to sum over μ such that $\mu_1 \leq \lambda_1$.

Let $C := \prod_{i\geq 1}(1-2^{-i})$ and $D := \frac{2}{1-2^{-1/8}}$. We apply Lemma 7.4,

$$\begin{aligned}\sum_{\mu} |G_{\mu,\lambda}| p^{\sum_i \frac{\mu_i'(\mu_i'-1)}{2}} &\leq \frac{1}{C^{\lambda_1}} \sum_{\mu, \mu_1 \leq \lambda_1} p^{\sum_{i=1}^{\lambda_1} \mu_i'\lambda_i' - (\mu_i')^2 + \frac{\mu_i'(\mu_i'-1)}{2}} \\ &= \frac{1}{C^{\lambda_1}} \sum_{d_1,\ldots,d_{\lambda_1} \geq 0} p^{\sum_{i=1}^{\lambda_1} d_i\lambda_i' - d_i^2 + \frac{d_i(d_i-1)}{2}} \\ &= \frac{p^{\sum_i \frac{\lambda_i'(\lambda_i'-1)}{2}}}{C^{\lambda_1}} \sum_{d_1,\ldots,d_{\lambda_1} \geq 0} (p^{\frac{1}{8}})^{\sum_{i=1}^{\lambda_1} -(2d_i - 2\lambda_i'+1)^2+1} \\ &\leq \frac{p^{\sum_i \frac{\lambda_i'(\lambda_i'-1)}{2}}}{C^{\lambda_1}} \sum_{e_1,\ldots,e_{\lambda_1} \in \mathbb{Z},\ e_i \text{ odd}} (p^{\frac{1}{8}})^{\sum_{i=1}^{\lambda_1} -e_i^2+1}.\end{aligned}$$

We have that

$$\sum_{e_1 \in \mathbb{Z},\ e_1 \text{ odd}} (p^{\frac{1}{8}})^{-e_1^2+1} \leq 2 \sum_{e_1 \geq 1} (p^{\frac{1}{8}})^{-e_1^2+1} \leq 2 \sum_{e_1 \geq 1} (p^{\frac{1}{8}})^{-e_1+1} = \frac{2}{1-p^{-1/8}} \leq D.$$

So, applying this to each of the λ_1 sums, we have

$$\sum_{G_1 \text{ subgroup of } G} |\wedge^2 G_1| \leq \frac{p^{\sum_i \frac{\lambda_i'(\lambda_i'-1)}{2}}}{C^{\lambda_1}} \sum_{e_1,\ldots,e_{\lambda_1}\in\mathbb{Z},\ e_i \text{ odd}} (p^{\frac{1}{8}})^{\sum_{i=1}^{\lambda_1} -e_i^2+1}$$
$$\leq \frac{p^{\sum_i \frac{\lambda_i'(\lambda_i'-1)}{2}}}{C^{\lambda_1}} D^{\lambda_1}. \qquad \square$$

The above lemma will be used in particular to see that our moments are not too big for the method developed in the next section to recover a distribution from its moments.

8. Moments determine the distribution

In this section we will see that the moments we have found in fact determine the distributions of our group valued random variables. We have been working with the moments $\mathbb{E}(\#\operatorname{Sur}(-,G))$ so far. As we have seen, these take nice values. Summing over all subgroups of G, we then obtain the moments $\mathbb{E}(\#\operatorname{Hom}(-,G))$. From the point of view of how we found these moments, the "Hom" moments are just derivative from the "Sur" moments. However, from an analytic point of view, the moments $\mathbb{E}(\#\operatorname{Hom}(-,G))$ are easier to work with. For example, if $G = (\mathbb{Z}/p\mathbb{Z})^k$ for a prime p, then $\#\operatorname{Hom}(H,G) = p^{(p\text{-rank}(H))k}$. So for $G = (\mathbb{Z}/p\mathbb{Z})^k$, the Hom moments give the usual moments of the random variable $p^{p\text{-rank}(H)}$. For example, when S is a sandpile group of a random graph, as above, we have that $\mathbb{E}(\left(p^{p\text{-rank}(S)}\right)^k)$ is on the order of $p^{k(k-1)/2}$ (see Lemma 7.5).

As discussed in the Introduction, these moments are too big to use Carleman's condition to recover the distribution, but we can take advantage of the fact that we know the random variable takes only values p^i, where i is a non-negative integer. In this case, we can view the problem as one of a countably infinite system of linear equations which we would like to show has a unique (non-negative) solution. Heath-Brown [HB94a, Lemma 17] (see also [HB94b, Lemma 17]) and Fouvry and Klüners [FK06, Section 4.2] have methods which will show that for $\mathbb{E}(\left(p^{p\text{-rank}(S)}\right)^k)$ on the order of $p^{k(k-1)/2}$, the moments do indeed determine the distribution of p-rank(S). (See also [EVW16, Lemma 8.1] for the case when all the Sur moments are 1.) However, this will at best determine the distribution of the p-ranks of the sandpile groups.

Since we would like to determine more than just the p-ranks of the sandpile group, in this section we prove that we can recover the distribution from the moments we have found. Heath-Brown's method [HB94a, Lemma 17] is to construct an infinite matrix that lower-triangularizes the infinite matrix that gives the relevant system of linear equations. Once the system is lower-triangular, it certainly has a unique solution. The difficulty is to construct a matrix with entries that are sufficiently small (and you can prove are sufficiently small) so that all the infinite sums involved converge. Heath-Brown constructs his matrix with entries from Taylor expansions of analytic functions in one variable.

Our approach is to develop a multi-variable version of Heath-Brown's method. However, the size of our moments are on the boundary of where this approach will work, and the functions we construct in the following lemma are carefully optimized. In particular, it is critical that only terms with $d_2 + \cdots + d_m \leq b_1$ appear in the

Taylor expansion of $H_{m,p,b}(z)$ below. We now construct the analytic functions of several variables whose Taylor coefficients we will use to lower-triangularize our system of equations.

Lemma 8.1. *Given a positive integer m, a prime p, and $b \in \mathbb{Z}^m$ with $b_1 \geq b_2 \geq \cdots \geq b_m$, we have an entire analytic function in the m variables $z_1, \ldots, z_m$*

$$H_{m,p,b}(z) = \sum_{\substack{d_1,\ldots,d_m \geq 0 \\ d_2+\cdots+d_m \leq b_1}} a_{d_1,\ldots,d_m} z_1^{d_1} \cdots z_m^{d_m}$$

and a constant E (depending on m, p, and b) such that

$$|a_{d_1,\ldots,d_m}| \leq E p^{-b_1 d_1 - \frac{d_1(d_1+1)}{2}}.$$

Further, if f is a partition of length at most m and $f > b$ (in the lexicographic ordering), then $H_{m,p,b}(p^{f_1}, p^{f_1+f_2}, \ldots, p^{f_1+\cdots+f_m}) = 0$. If $f = b$, then $H_{m,p,b}(p^{f_1}, p^{f_1+f_2}, \ldots, p^{f_1+\cdots+f_m}) \neq 0$.

Note that we could make E explicit in the proof below, but we do not for simplicity.

Proof. We define analytic functions

$$G(z_1) := \prod_{j \geq b_1+1} \left(1 - \frac{z_1}{p^j}\right) = \sum_{d_1 \geq 0} c_{d_1} z_1^{d_1}$$

and

$$\begin{aligned} &H(z_2, \ldots, z_m) \\ &:= \prod_{j=b_1+b_2+1}^{2b_1} \left(1 - \frac{z_2}{p^j}\right) \prod_{j=b_1+b_2+b_3+1}^{b_1+2b_2} \left(1 - \frac{z_3}{p^j}\right) \cdots \prod_{j=b_1\cdots+b_m+1}^{b_1+\cdots+b_{m-2}+2b_{m-1}} \left(1 - \frac{z_m}{p^j}\right) \\ &= \sum_{d_2,\ldots,d_m \geq 0} e_{d_2,\ldots,d_m} z_2^{d_2} \cdots z_m^{d_m}. \end{aligned}$$

In each of the z_i separately, for $2 \leq i \leq m$, we have that H is a polynomial of degree $b_{i-1} - b_i$. We then have an entire, analytic function in m variables

$$H_{m,p,b}(z) := G(z_1)H(z_2, \ldots, z_m) = \sum_{\substack{d_1,\ldots,d_m \geq 0 \\ d_2+\cdots+d_m \leq b_1}} a_{d_1,\ldots,d_m} z_1^{d_1} \cdots z_m^{d_m}.$$

We now estimate the size of the $a_{d_1,\ldots,d_m}$. We see that $a_{d_1,\ldots,d_m} = c_{d_1} e_{d_2,\ldots,d_m}$. We have that $G(pz) = (1 - \frac{z}{p^{b_1}})G(z)$. So $c_n p^n = c_n - p^{-b_1} c_{n-1}$. Thus $c_n = -\frac{p^{-b_1} c_{n-1}}{p^n - 1}$, and by induction, $c_n = (-1)^n \frac{p^{-b_1 n}}{\prod_{i=1}^n (p^i - 1)}$. So $|c_n| \leq p^{-b_1 n - \frac{n(n+1)}{2}} \prod_{i \geq 1} (1 - p^{-i})^{-1}$. Thus,

$$|a_{d_1,\ldots,d_m}| \leq \frac{1}{\prod_{i \geq 1}(1 - p^{-i})} p^{-b_1 d_1 - \frac{d_1(d_1+1)}{2}} \max_{d_2,\ldots,d_m} e_{d_2,\ldots,d_m}.$$

Now we check the final statements of the lemma. If $f > b$, suppose $f_i = b_i$ for $i \leq t$ and $f_{t+1} > b_{t+1}$ for some $0 \leq t \leq m-1$. Then, in particular, $f_1 + \cdots + f_i = b_1 + \cdots + b_i$ for $i \leq t$, and $f_1 + \cdots + f_{t+1} \geq b_1 + \cdots + b_{t+1} + 1$. However, (when $t \geq 1$) since $f_{t+1} \leq f_t = b_t$, we have $f_1 + \cdots + f_{t+1} \leq b_1 + \cdots + b_{t-1} + 2b_t$. Since $H_{m,p,b}$ vanishes whenever $z_{t+1} = p^k$ for integers k with $b_1 + \cdots + b_{t+1} + 1 \leq k \leq b_1 + \cdots + b_{t-1} + 2b_t$, we obtain the desired vanishing.

For the last statement, we first note that since the product in the definition of G is absolutely convergent, we have that $z_1 = p^{b_1}$ is not a root of G. Then we observe all the other finitely many factors in H are non-zero in this case as well. □

In the following theorem, we prove that the variation of the moments, in which we take all homomorphisms instead of just surjections, of our abelian group valued random variables determines the distribution of the variables when the moments are not too large. We state the result in terms of an infinite system of linear equations. We will apply this with C_λ, the expected number of homomorphisms, to a group of type λ, and x_μ and y_μ are the probabilities that the random variable is a group of type μ. Note that the expected number of homomorphisms is a mixed moment, in the traditional sense, of the variables $p_j^{\mu_i^j}$.

Theorem 8.2. *Let $p_1, \dots, p_s$ be distinct primes. Let $m_1, \dots, m_s \geq 1$ be integers. Let M_j be the set of partitions λ with at most m_j parts. Let $M = M_1 \times \cdots \times M_s$. For $\mu \in M$, we write μ^j for its jth entry, which is a partition consisting of non-negative integers μ_i^j with $\mu_1^j \geq \mu_2^j \geq \cdots \mu_{m_j}^j$. Suppose we have non-negative reals x_μ, y_μ, for each tuple of partitions $\mu \in M$. Further suppose that we have non-negative reals C_λ for each $\lambda \in M$ such that*

$$C_\lambda \leq \prod_{j=1}^{s} F^{m_j} p_j^{\sum_i \frac{\lambda_i^j(\lambda_i^j-1)}{2}},$$

where $F > 0$ is an absolute constant. Suppose that for all $\lambda \in M$,

$$\sum_{\mu \in M} x_\mu \prod_{j=1}^{s} p_j^{\sum_i \lambda_i^j \mu_i^j} = \sum_{\mu \in M} y_\mu \prod_{j=1}^{s} p_j^{\sum_i \lambda_i^j \mu_i^j} = C_\lambda. \tag{7}$$

Then for all μ, we have that $x_\mu = y_\mu$.

To prove Theorem 8.2, we will use the analytic functions constructed in Lemma 8.1 to construct an infinite matrix that will lower-triangularize the system of equations in (7) below.

Proof. We will induct on the size of μ in the lexicographic total ordering (we take the lexicographic ordering for partitions and then the lexicographic ordering on top of that for tuples of partitions). Suppose for a $\nu \in M$ have $x_\pi = y_\pi$ for every $\pi \in M$ with $\pi < \nu$.

We use Lemma 8.1 to find $H_{m_j, p_j, \nu^j}(z) = \sum_d a(j)_d z_1^{d_1} \cdots z_{m_j}^{d_{m_j}}$. For $\lambda \in M$, we define

$$A_\lambda := \prod_{j=1}^{s} a(j)_{\lambda_1^j - \lambda_2^j, \lambda_2^j - \lambda_3^j, \dots, \lambda_{m_j}^j}.$$

We wish to show that the sum $\sum_{\lambda \in M} A_\lambda C_\lambda$ converges absolutely. We have

$$\begin{aligned} \sum_{\lambda \in M} |A_\lambda C_\lambda| &\leq \sum_{\lambda \in M} \prod_{j=1}^{s} \left| a(j)_{\lambda_1^j - \lambda_2^j, \lambda_2^j - \lambda_3^j, \dots, \lambda_{m_j}^j} F^{m_j} p_j^{\sum_i \frac{\lambda_i^j(\lambda_i^j-1)}{2}} \right| \\ &= \prod_{j=1}^{s} \sum_{\lambda \in M_j} \left| a(j)_{\lambda_1 - \lambda_2, \lambda_2 - \lambda_3, \dots, \lambda_{m_j}} F^{m_j} p_j^{\sum_i \frac{\lambda_i(\lambda_i-1)}{2}} \right|. \end{aligned}$$

We now investigate the inner sum. We drop the j index, and let $b = \nu^j$. We apply Lemma 8.1 to obtain

$$\sum_{\substack{d_1,\dots,d_m\geq 0\\ d_2+\cdots+d_m\leq b_1}} |a(j)_{d_1,d_2,\dots,d_m}| F^m p^{\sum_i \frac{\sum_{k=i}^m d_k(\sum_{k=i}^m d_k-1)}{2}}$$
$$\leq \sum_{\substack{d_1,\dots,d_m\geq 0\\ d_2+\cdots+d_m\leq b_1}} Ep^{-b_1 d_1-\frac{d_1(d_1+1)}{2}} F^m p^{\sum_i \frac{\sum_{k=i}^m d_k(\sum_{k=i}^m d_k-1)}{2}}.$$

For each choice of $d_2,\dots,d_m$, the remaining sum over d_1 is a constant times $\sum_{d_1\geq 0} p^{d_1(-b_1-1+d_2+\cdots+d_m)}$, which converges, so it follows that $\sum_{\lambda\in M} A_\lambda C_\lambda$ converges absolutely.

Suppose we have x_μ for $\mu\in M$ all non-negative, such that for all $\lambda\in M$,

$$\sum_{\mu\in M} x_\mu \prod_{j=1}^s p_j^{\sum_i \lambda_i^j\mu_i^j} = C_\lambda.$$

So we have that

$$\sum_{\lambda\in M}\sum_{\mu\in M} A_\lambda x_\mu \prod_{j=1}^s p_j^{\sum_i \lambda_i^j\mu_i^j}$$

converges absolutely. Thus,

$$\begin{aligned}\sum_{\lambda\in M} A_\lambda C_\lambda &= \sum_{\lambda\in M}\sum_{\mu\in M} A_\lambda x_\mu \prod_{j=1}^s p_j^{\sum_i \lambda_i^j\mu_i^j}\\ &= \sum_{\mu\in M} x_\mu \sum_{\lambda\in M} A_\lambda \prod_{j=1}^s p_j^{\sum_i \lambda_i^j\mu_i^j}\\ &= \sum_{\mu\in M} x_\mu \prod_{j=1}^s \sum_{\lambda\in M_j} a(j)_{\lambda_1-\lambda_2,\lambda_2-\lambda_3,\dots,\lambda_{m_j}} p_j^{\sum_i \lambda_i^j\mu_i^j}.\end{aligned}$$

Now we consider the inner sum. Again we drop the j indices. We have

$$\begin{aligned}&\sum_{\lambda\in M_j} a(j)_{\lambda_1-\lambda_2,\lambda_2-\lambda_3,\dots,\lambda_m} p^{\sum_i \lambda_i\mu_i}\\ &= \sum_{d_1,\dots,d_m\geq 0} a(j)_{d_1,\dots,d_m} (p^{\mu_1})^{d_1}(p^{\mu_1+\mu_2})^{d_2}\cdots(p^{\mu_1+\cdots+\mu_m})^{d_m}\\ &= H_{m,p,\nu}(p^{\mu_1}, p^{\mu_1+\mu_2},\dots,p^{\mu_1+\cdots+\mu_m}).\end{aligned}$$

If $\mu>\nu$ (in the lexicographic total ordering), then some $\mu^j>\nu^j$, and so for $m=m_j$ and $p=p_j$, by Lemma 8.1, $H_{m,p,\nu^j}(p^{\mu_1}, p^{\mu_1+\mu_2},\dots,p^{\mu_1+\cdots+\mu_m})=0$. Further, if $\mu=\nu$, then for each (implicit) j we have $H_{m,p,\nu}(p^{\mu_1}, p^{\mu_1+\mu_2},\dots,p^{\mu_1+\cdots+\mu_m})\neq 0$. So for some non-zero u,

$$\sum_{\lambda\in M} A_\lambda C_\lambda = x_\nu u + \sum_{\mu\in M,\mu<\nu} x_\mu \sum_{\lambda\in M} A_\lambda \prod_{j=1}^s p_j^{\sum_i \lambda_i^j\mu_i^j}.$$

So since by assumption x_μ with $\mu<\nu$ we determined by the C_λ, we conclude that x_ν is determined as well. □

In the following theorem we achieve two things. We translate solving the above studied system of linear equations into finding the distribution of our random groups given their moments. We also deal with the issue that we do not technically have moments of a distribution, but rather limits of moments of a sequence of distributions. An important ingredient in solving this issue is showing that in our case, for any particular equation, we can use bounds coming from other equations to show that we satisfy the hypotheses of the Lebesgue dominated convergence theorem.

Theorem 8.3. *Let X_n be a sequence of random variables taking values in finitely generated abelian groups. Let a be a positive integer and A be the set of (isomorphism classes of) abelian groups with exponent dividing a. Suppose that for every $G \in A$, we have*

$$\lim_{n\to\infty} \mathbb{E}(\#\operatorname{Sur}(X_n, G)) = |\wedge^2 G|.$$

Then for every $H \in A$, the limit $\lim_{n\to\infty} \mathbb{P}(X_n \otimes \mathbb{Z}/a\mathbb{Z} \simeq H)$ exists, and for all $G \in A$ we have

$$\sum_{H\in A} \lim_{n\to\infty} \mathbb{P}(X_n \otimes \mathbb{Z}/a\mathbb{Z} \simeq H)\#\operatorname{Sur}(H, G) = |\wedge^2 G|.$$

Suppose Y_n is a sequence of random variables taking values in finitely generated abelian groups such that for every $G \in A$, we have

$$\lim_{n\to\infty} \mathbb{E}(\#\operatorname{Sur}(Y_n, G)) = |\wedge^2 G|.$$

Then, we have that for every $H \in A$

$$\lim_{n\to\infty} \mathbb{P}(X_n \otimes \mathbb{Z}/a\mathbb{Z} \simeq H) = \lim_{n\to\infty} \mathbb{P}(Y_n \otimes \mathbb{Z}/a\mathbb{Z} \simeq H).$$

Proof. First, we will suppose that the limits $\lim_{n\to\infty} \mathbb{P}(X_n \otimes \mathbb{Z}/a\mathbb{Z} \simeq H)$ exist, and from that we show that

$$\sum_{H\in A} \lim_{n\to\infty} \mathbb{P}(X_n \otimes \mathbb{Z}/a\mathbb{Z} \simeq H)\#\operatorname{Sur}(H, G) = |\wedge^2 G|.$$

For each $G \in A$, we claim we can find an abelian group $G' \in A$ such that

$$\sum_{H\in A} \frac{\#\operatorname{Hom}(H, G)}{\#\operatorname{Hom}(H, G')}$$

converges. We can factor over the primes p dividing a and reduce to the problem when $a = p^e$. Then if G has type λ, we take G' of type π with $\pi'_i = 2\lambda'_i + 1$ for $1 \le i \le e$. Then we use Lemma 7.1 and we see

$$\sum_{c_1\ge\cdots\ge c_e\ge 0} p^{\sum_{i=1}^e c_i(\lambda'_i - 2\lambda'_i - 1)} = \sum_{c_1\ge\cdots\ge c_e\ge 0} p^{\sum_{i=1}^e c_i(-\lambda'_i - 1)}$$

converges.

We have

$$\begin{aligned}\sum_{B\in A} \mathbb{P}(X_n \otimes \mathbb{Z}/a\mathbb{Z} \simeq B)\#\operatorname{Hom}(B, G') &= \mathbb{E}(\#\operatorname{Hom}(X_n, G')) \\ &= \sum_{H\subset G'} \mathbb{E}(\#\operatorname{Sur}(X_n, H)),\end{aligned}$$

and by supposition, each of the finite summands on the right-hand side has a finite limit as $n \to \infty$ (and in particular is bounded above for all n). Thus, there is some constant D_G such that for all n we have

$$\mathbb{P}(X_n \otimes \mathbb{Z}/a\mathbb{Z} \simeq H)\#\operatorname{Hom}(H, G') \leq \sum_{B \in A} \mathbb{P}(X_n \otimes \mathbb{Z}/a\mathbb{Z} \simeq B)\#\operatorname{Hom}(B, G') \leq D_G.$$

Thus, for all n,

$$\mathbb{P}(X_n \otimes \mathbb{Z}/a\mathbb{Z} \simeq H)\#\operatorname{Hom}(H, G) \leq D_G\#\operatorname{Hom}(H, G)\#\operatorname{Hom}(H, G')^{-1}.$$

Since $\sum_{H \in A} D_G\#\operatorname{Hom}(H, G)\#\operatorname{Hom}(H, G')^{-1}$ converges, by the Lebesgue dominated convergence theorem we have

$$\begin{aligned}&\sum_{H \in A} \lim_{n \to \infty} \mathbb{P}(X_n \otimes \mathbb{Z}/a\mathbb{Z} \simeq H)\#\operatorname{Hom}(H, G)\\ &\quad = \lim_{n \to \infty} \sum_{H \in A} \mathbb{P}(X_n \otimes \mathbb{Z}/a\mathbb{Z} \simeq H)\#\operatorname{Hom}(H, G).\end{aligned}$$

As this holds for every $G \in A$, we also have (by a finite number of additions and subtractions)

$$\begin{aligned}&\sum_{H \in A} \lim_{n \to \infty} \mathbb{P}(X_n \otimes \mathbb{Z}/a\mathbb{Z} \simeq H)\#\operatorname{Sur}(H, G)\\ &\quad = \lim_{n \to \infty} \sum_{H \in A} \mathbb{P}(X_n \otimes \mathbb{Z}/a\mathbb{Z} \simeq H)\#\operatorname{Sur}(H, G)\\ &\quad = |\wedge^2 G|.\end{aligned}$$

Next, we show that if for every $G \in A$,

$$\begin{aligned}&\sum_{H \in A} \lim_{n \to \infty} \mathbb{P}(X_n \otimes \mathbb{Z}/a\mathbb{Z} \simeq H)\#\operatorname{Sur}(H, G)\\ &\quad = \sum_{H \in A} \lim_{n \to \infty} \mathbb{P}(Y_n \otimes \mathbb{Z}/a\mathbb{Z} \simeq H)\#\operatorname{Sur}(H, G)\\ &\quad = |\wedge^2 G|,\end{aligned}$$

then we have for every $H \in A$ that $\lim_{n \to \infty} \mathbb{P}(X_n \otimes \mathbb{Z}/a\mathbb{Z} \simeq H) = \lim_{n \to \infty} \mathbb{P}(Y_n \otimes \mathbb{Z}/a\mathbb{Z} \simeq H)$. For each G, by a finite number of additions we have

$$\begin{aligned}&\sum_{H \in A} \lim_{n \to \infty} \mathbb{P}(X_n \otimes \mathbb{Z}/a\mathbb{Z} \simeq H)\#\operatorname{Hom}(H, G)\\ &\quad = \sum_{H \in A} \lim_{n \to \infty} \mathbb{P}(Y_n \otimes \mathbb{Z}/a\mathbb{Z} \simeq H)\#\operatorname{Hom}(H, G)\\ &\quad = \sum_{G_1 \text{ subgroup of } G} |\wedge^2 G_1|.\end{aligned}$$

Now we will explain how to apply Theorem 8.2 to conclude that $\lim_{n \to \infty} \mathbb{P}(X_n \otimes \mathbb{Z}/a\mathbb{Z} \simeq H) = \lim_{n \to \infty} \mathbb{P}(Y_n \otimes \mathbb{Z}/a\mathbb{Z} \simeq H)$. We factor $a = \prod_{j=1}^{s} p_j^{m_j}$. The partition $\lambda^j \in M_j$ is the transpose of the type of the Sylow p_j-subgroup of H, which gives a bijection between M and A. We have that for $G \in A$ with corresponding $\lambda \in M$,

$$C_\lambda = \sum_{G_1 \text{ subgroup of } G} |\wedge^2 G_1| \leq \prod_{j=1}^{s} F^{m_j} p_j^{\sum_i \frac{\lambda_i^j(\lambda_i^j - 1)}{2}},$$

by Lemma 7.5. For $H, G \in A$ with corresponding $\mu, \lambda \in M$, we have $\#\operatorname{Hom}(H,G) = \prod_{j=1}^{s} p_j^{\sum_i \lambda_i^j \mu_i^j}$. So for $H \in A$ with corresponding $\mu \in M$, we let $x_\mu := \lim_{n\to\infty} \mathbb{P}(X_n \otimes \mathbb{Z}/a\mathbb{Z} \simeq H)$ and similarly for y_μ, and we can apply Theorem 8.2.

Now, we suppose for the sake of contradiction that the limit $\lim_{n\to\infty} \mathbb{P}(X_n \otimes \mathbb{Z}/a\mathbb{Z} \simeq H)$ does not exist for at least some $H \in A$. Then we can use a diagonal argument to find a subsequence of X_n where the limits do exist for all $H \in A$, and then another subsequence where the limits do also exist for all $H \in A$, but at least one is different. In each subsequence the limits $\lim_{n\to\infty} \mathbb{P}(X_{i_n} \otimes \mathbb{Z}/a\mathbb{Z} \simeq H)$ exist. Above, we have shown that if these limits exist, then the limit probabilities give the $|\wedge^2 G|$ moments. We can apply that to each of our subsequences. But above we have also shown that if we have two sequences whose limit probabilities give the $|\wedge^2 G|$ moments, they have the same limit probabilities, a contradiction of our choice of subsequences. □

9. Comparison to uniform random matrices

Above we have seen that the moments we have determined for sandpile groups of random graphs in particular imply many well-defined asymptotic statistics of the sandpile groups, but we have not yet determined the values of these statistics. From Theorem 6.1 we see these same moments hold for cokernels of a wide class of random matrices, in particular uniform random matrices over $\mathbb{Z}/a\mathbb{Z}$. (Though the moments for cokernels of uniform random matrices follow from Theorem 6.1, there is a much simpler proof for the uniform case given in [CLK+14].) We can then use computations in the uniform case to give us our desired statistics.

Corollary 9.1 (of Theorems 1.2, 6.1, and 8.3)**.** *Let G be a finite abelian group of exponent dividing a. Let $\Gamma \in G(n,q)$ be a random graph with sandpile group S. Let H_n be a uniform random $n \times n$ symmetric matrix with entries in $\mathbb{Z}/a\mathbb{Z}$.*

$$\lim_{n\to\infty} \mathbb{P}(S \otimes \mathbb{Z}/a\mathbb{Z} \simeq G) = \lim_{n\to\infty} \mathbb{P}(\operatorname{cok}(H_n) \simeq G).$$

In particular, we can conclude the following, which proves Theorem 1.1.

Corollary 9.2. *Let G be a finite abelian group. Let $\Gamma \in G(n,q)$ be a random graph with sandpile group S. Let P be a finite set of primes including all those dividing $|G|$. Let H_n be a random $n \times n$ symmetric matrix with entries in $\prod_{p\in P} \mathbb{Z}_p$ with respect to Haar measure. Let S_P be the sum of the Sylow p-subgroups of S for $p \in P$. Then*

$$\begin{aligned}
&\lim_{n\to\infty} \mathbb{P}(S_P \simeq G) \\
&\quad = \lim_{n\to\infty} \mathbb{P}(\operatorname{cok}(H_n) \simeq G) \\
&\quad = \frac{\#\{\textit{symmetric, bilinear, perfect } \phi : G \times G \to \mathbb{C}^*\}}{|G||\operatorname{Aut}(G)|} \prod_{p\in P} \prod_{k\geq 0} (1 - p^{-2k-1}).
\end{aligned}$$

Proof. Note that if G is a finite abelian group with an exponent that has prime factorization $\prod_{p\in P} p^{e_p}$, then if we take $a = \prod_{p\in P} p^{e_p+1}$, for any finitely generated abelian group H, with H_P the sum of the Sylow p-subgroups of H for $p \in P$, we have

$$H \otimes \mathbb{Z}/a\mathbb{Z} \simeq G \text{ if and only if } H_P \simeq G.$$

So the first equality follows from Corollary 9.1.

For the second equality, note that everything factors over $p \in P$, and so we can reduce to the case when G is a p-group. Let Φ_G be the set of symmetric, bilinear, perfect pairings $\phi : G \times G \to \mathbb{C}^*$. For $\phi \in \Phi_G$, we let $\mathrm{Aut}(G, \phi)$ be the set of automorphisms of G that respect the pairing ϕ. Then $\mathrm{Aut}(G)$ acts naturally on Φ_G, with orbits the isomorphism classes of symmetric, bilinear, perfect pairings $G \times G \to \mathbb{C}^*$, and stabilizers $\mathrm{Aut}(G, \phi)$ for ϕ in the isomorphism class. Let $\bar{\Phi}_G$ be the set of isomorphism classes of symmetric, bilinear, perfect pairings $G \times G \to \mathbb{C}^*$.

Then [CLK+14, Theorem 2] shows that

$$\lim_{n\to\infty} \mathbb{P}(\mathrm{cok}(H_n) \simeq G) = \sum_{[\phi]\in\bar{\Phi}_G} \frac{1}{|G||\mathrm{Aut}(G,\phi)|} \prod_{k\geq 0}(1 - p^{-2k-1}).$$

By the orbit-stabilizer theorem, we have

$$\sum_{[\phi]\in\bar{\Phi}_G} \frac{1}{\#\mathrm{Aut}(G,\phi)} = \sum_{\phi\in\Phi_G} \frac{1}{|\mathrm{Aut}(G)|}.$$

We conclude the second equality of the corollary. □

In particular, this lets us see that any particular group appears asymptotically with probability 0.

Corollary 9.3. *Let G be a finite abelian group. Let $\Gamma \in G(n, q)$ be a random graph with sandpile group S. Then*

$$\lim_{n\to\infty} \mathbb{P}(S \simeq G) = 0.$$

Proof. Let P_N be the set of primes $\leq N$ *not* dividing the order of G. Let S_N be the sum of the Sylow p-subgroups of S for $p \in P_N$. Then

$$\lim_{n\to\infty} \mathbb{P}(S \simeq G) \leq \lim_{n\to\infty} \mathbb{P}(S_N \text{ trival}) = \prod_{p\in P_N} \prod_{k\geq 0}(1 - p^{-2k-1}),$$

where the last equality is by Corollary 9.2. In particular, since the product $\prod_{p\in P_N}(1 - p^{-1})$ goes to 0 as $N \to \infty$, we can conclude the corollary. □

Also taking $a = p$ for a prime p in Corollary 9.1, we conclude the following on the distribution of p-ranks of sandpile groups.

Corollary 9.4. *Let p be a prime. Let $\Gamma \in G(n, q)$ be a random graph with sandpile group S. Let H_n be a uniform random $n \times n$ symmetric matrix with entries in $\mathbb{Z}/p\mathbb{Z}$. Then for every non-negative integer r*

$$\begin{aligned}\lim_{n\to\infty} \mathbb{P}(\mathrm{rank}(S \otimes \mathbb{Z}/p\mathbb{Z}) = r) &= \lim_{n\to\infty} \mathbb{P}(\mathrm{rank}(H_n) = n - r) \\ &= p^{-\frac{r(r+1)}{2}} \prod_{i=r+1}^{\infty}(1 - p^{-i}) \prod_{i=1}^{\infty}(1 - p^{-2i})^{-1}.\end{aligned}$$

Proof. We have the second equality because the number of symmetric $n\times n$ matrices over $\mathbb{Z}/p\mathbb{Z}$ with rank $n - r$ is (by [Mac69, Theorem 2]) $p^{\frac{n(n+1)}{2} - \frac{r(r+1)}{2}} \prod_{i=1}^{\lfloor (n-r)/2 \rfloor}(1 - p^{-2i})^{-1} \prod_{i=r+1}^{n}(1 - p^{-i})$. □

We can also conclude an asymptotic upper bound on the probability that the sandpile group is cyclic.

Corollary 9.5. *Let $\Gamma \in G(n,q)$ be a random graph with sandpile group S. Then*

$$\lim_{n\to\infty} \mathbb{P}(S \text{ cyclic}) \leq \zeta(3)^{-1}\zeta(5)^{-1}\zeta(7)^{-1}\zeta(9)^{-1}\cdots.$$

Proof. Let P_N be the set of primes $\leq N$. Let S_N be the sum of the Sylow p-subgroups of S for $p \in P_N$. Then

$$\lim_{n\to\infty} \mathbb{P}(S \text{ cyclic}) \leq \lim_{n\to\infty} \mathbb{P}(S_N \text{ cyclic}).$$

We apply Corollary 9.1 with a the product of the primes in P_N and add over all G cyclic with exponent dividing a. We have

$$\sum_{G \text{ cyclic}, aG=0} \mathbb{P}(\operatorname{cok}(H_n) \simeq G) = \prod_{p\in P_N} \left(\mathbb{P}(\operatorname{cok}(H_n(\bmod p)) \simeq 1) + \mathbb{P}(\operatorname{cok}(H_n(\bmod p)) \simeq \mathbb{Z}/p\mathbb{Z})\right).$$

By [Mac69, Theorem 2], as above, we have

$$\begin{aligned}
&\lim_{n\to\infty} \left(\mathbb{P}(\operatorname{cok}(H_n(\bmod p))) \simeq 1) + \mathbb{P}(\operatorname{cok}(H_n(\bmod p))) \simeq \mathbb{Z}/p\mathbb{Z})\right)\\
=&\prod_{i=1}^{\infty}(1-p^{-2i})^{-1}\prod_{i=1}^{\infty}(1-p^{-i}) + p^{-1}\prod_{i=1}^{\infty}(1-p^{-2i})^{-1}\prod_{i=2}^{\infty}(1-p^{-i})\\
=&\prod_{i=1}^{\infty}(1-p^{-2i-1}).
\end{aligned}$$

So,

$$\lim_{n\to\infty} \mathbb{P}(S \text{ cyclic}) \leq \prod_{p\in P_N}\prod_{i=1}^{\infty}(1-p^{-2i-1}).$$

Taking the limit as $N \to \infty$, we obtain the corollary. □

Similarly, we can obtain an asymptotic upper bound for the probability that the number of spanning trees is square-free.

Corollary 9.6. *Let $\Gamma \in G(n,q)$ be a random graph with sandpile group S. Then*

$$\lim_{n\to\infty} \mathbb{P}(|S| \textit{ square-free}) \leq \zeta(2)^{-1}\zeta(3)^{-1}\zeta(5)^{-1}\zeta(7)^{-1}\zeta(9)^{-1}\cdots.$$

Proof. Let P_N be the set of primes $\leq N$. Let S_N be the sum of the Sylow p-subgroups of S for $p \in P_N$. Then

$$\lim_{n\to\infty} \mathbb{P}(|S| \text{ square-free}) \leq \lim_{n\to\infty} \mathbb{P}(|S_N| \text{ square-free}).$$

By summing Corollary 9.2 over all G such that $|G|$ has all prime factors in P_N and $|G|$ is square-free, we have

$$\begin{aligned}
\lim_{n\to\infty} \mathbb{P}(|S_N| \text{ square-free}) &= \prod_{p\in P_N}\left((1+p^{-1})\prod_{k\geq 0}(1-p^{-2k-1})\right)\\
&= \prod_{p\in P_N}\left((1-p^{-2})\prod_{k\geq 1}(1-p^{-2k-1})\right).
\end{aligned}$$

Taking the limit as $N \to \infty$, we obtain the corollary. □

Remark 9.7. Of course, all of the corollaries in this section also follow if S is replaced by the cokernel of a random matrix satisfying the hypotheses of Theorem 6.1 (using Theorem 6.1 in place of Theorem 1.2).

It would be nice to know the rest of the limits for uniform random matrices that occur in Corollary 9.1. More specifically, let H_n be a uniform random $n \times n$ symmetric matrix with entries in $\mathbb{Z}/a\mathbb{Z}$. What is

$$\lim_{n\to\infty} \mathbb{P}(\mathrm{cok}(H_n) \simeq G)?$$

Above we have seen the answer when a is a prime, and when every prime dividing the exponent of G divides a to at least one higher power than it divides the exponent of G.

Acknowledgment

The author would like to thank Sam Payne, Betsy Stovall, Jordan Ellenberg, Philip Matchett Wood, Benedek Valko, and Steven Sam for useful conversations regarding the work in this paper, and Sam Payne, Philip Matchett Wood, Lionel Levine, Van Vu, Dino Lorenzini, Karola Mészáros, and the referees for helpful comments on the exposition.

References

[AV12] Carlos A. Alfaro and Carlos E. Valencia, *On the sandpile group of the cone of a graph*, Linear Algebra Appl. **436** (2012), no. 5, 1154–1176, DOI 10.1016/j.laa.2011.07.030. MR2890910

[BdlHN97] Roland Bacher, Pierre de la Harpe, and Tatiana Nagnibeda, *The lattice of integral flows and the lattice of integral cuts on a finite graph* (English, with English and French summaries), Bull. Soc. Math. France **125** (1997), no. 2, 167–198. MR1478029

[Bai97] Z. D. Bai, *Circular law*, Ann. Probab. **25** (1997), no. 1, 494–529, DOI 10.1214/aop/1024404298. MR1428519

[BS10] Zhidong Bai and Jack W. Silverstein, *Spectral Analysis of Large Dimensional Random Matrices*, 2nd ed., Springer Series in Statistics, Springer, New York, 2010. MR2567175

[Bal68] G. V. Balakin, *The distribution of the rank of random matrices over a finite field* (Russian, with English summary), Teor. Veroyatn. Primen. **13** (1968), 631–641. MR0243571

[Bha05] Manjul Bhargava, *The density of discriminants of quartic rings and fields*, Ann. of Math. (2) **162** (2005), no. 2, 1031–1063, DOI 10.4007/annals.2005.162.1031. MR2183288

[BKLj+13] Manjul Bhargava, Daniel M. Kane, Lenstra Hendrik W., Bjorn Poonen, and Eric Rains, *Modeling the distribution of ranks, Selmer groups, and Shafarevich-Tate groups of elliptic curves*, Camb. J. Math. **3** (2015), no. 3, 275–321, DOI 10.4310/CJM.2015.v3.n3.a1. MR3393023

[Big97] Norman Biggs, *Algebraic potential theory on graphs*, Bull. Lond. Math. Soc. **29** (1997), no. 6, 641–682, DOI 10.1112/S0024609397003305. MR1468054

[Big99] N. L. Biggs, *Chip-firing and the critical group of a graph*, J. Algebraic Combin. **9** (1999), no. 1, 25–45, DOI 10.1023/A:1018611014097. MR1676732

[BKW97] Johannes Blömer, Richard Karp, and Emo Welzl, *The rank of sparse random matrices over finite fields*, Random Structures Algorithms **10** (1997), no. 4, 407–419, DOI 10.1002/(SICI)1098-2418(199707)10:4⟨407::AID-RSA1⟩3.0.CO;2-Y. MR1608234

[BL02] Siegfried Bosch and Dino Lorenzini, *Grothendieck's pairing on component groups of Jacobians*, Invent. Math. **148** (2002), no. 2, 353–396, DOI 10.1007/s002220100195. MR1906153

[BLS91] Anders Björner, László Lovász, and Peter W. Shor, *Chip-firing games on graphs*, European J. Combin. **12** (1991), no. 4, 283–291, DOI 10.1016/S0195-6698(13)80111-4. MR1120415

[BN07] Matthew Baker and Serguei Norine, *Riemann-Roch and Abel-Jacobi theory on a finite graph*, Adv. Math. **215** (2007), no. 2, 766–788, DOI 10.1016/j.aim.2007.04.012. MR2355607

[BN09] Matthew Baker and Serguei Norine, *Harmonic morphisms and hyperelliptic graphs*, Int. Math. Res. Not. IMRN **15** (2009), 2914–2955, DOI 10.1093/imrn/rnp037. MR2525845

[BM87] Richard P. Brent and Brendan D. McKay, *Determinants and ranks of random matrices over Z_m*, Discrete Math. **66** (1987), no. 1-2, 35–49, DOI 10.1016/0012-365X(87)90117-8. MR900928

[BTW88] Per Bak, Chao Tang, and Kurt Wiesenfeld, *Self-organized criticality*, Phys. Rev. A (3) **38** (1988), no. 1, 364–374, DOI 10.1103/PhysRevA.38.364. MR949160

[BVW10] Jean Bourgain, Van H. Vu, and Philip Matchett Wood, *On the singularity probability of discrete random matrices*, J. Funct. Anal. **258** (2010), no. 2, 559–603, DOI 10.1016/j.jfa.2009.04.016. MR2557947

[But87] Lynne M. Butler, *A unimodality result in the enumeration of subgroups of a finite abelian group*, Proc. Amer. Math. Soc. **101** (1987), no. 4, 771–775, DOI 10.2307/2046687. MR911049

[CL84] H. Cohen and H. W. Lenstra Jr., *Heuristics on Class Groups of Number Fields*, Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983), Lecture Notes in Math., vol. 1068, Springer, Berlin, 1984, pp. 33–62, DOI 10.1007/BFb0099440. MR756082

[CLK+14] Julien Clancy, Nathan Kaplan, Timothy Leake, Sam Payne, and Melanie Matchett Wood, *On a Cohen-Lenstra heuristic for Jacobians of random graphs*, J. Algebraic Combin. **42** (2015), no. 3, 701–723, DOI 10.1007/s10801-015-0598-x. MR3403177

[CLP13] Julien Clancy, Timothy Leake, and Sam Payne, *A note on Jacobians, Tutte polynomials, and two-variable zeta functions of graphs*, Exp. Math. **24** (2015), no. 1, 1–7, DOI 10.1080/10586458.2014.917443. MR3305035

[CM90] Henri Cohen and Jacques Martinet, *Étude heuristique des groupes de classes des corps de nombres* (French), J. Reine Angew. Math. **404** (1990), 39–76. MR1037430

[Coo00] C. Cooper, *On the rank of random matrices*, Random Structures Algorithms **16** (2000), no. 2, 209–232, DOI 10.1002/(SICI)1098-2418(200003)16:2⟨209::AID-RSA6⟩3.3.CO;2-T. MR1742352

[Cos13] Kevin P. Costello, *Bilinear and quadratic variants on the Littlewood-Offord problem*, Israel J. Math. **194** (2013), no. 1, 359–394, DOI 10.1007/s11856-012-0082-4. MR3047075

[CSX14] David B. Chandler, Peter Sin, and Qing Xiang, *The Smith and critical groups of Paley graphs*, J. Algebraic Combin. **41** (2015), no. 4, 1013–1022, DOI 10.1007/s10801-014-0563-0. MR3342710

[CTV06] Kevin P. Costello, Terence Tao, and Van Vu, *Random symmetric matrices are almost surely nonsingular*, Duke Math. J. **135** (2006), no. 2, 395–413, DOI 10.1215/S0012-7094-06-13527-5. MR2267289

[CRR90] Leonard S. Charlap, Howard D. Rees, and David P. Robbins, *The asymptotic probability that a random biased matrix is invertible*, Discrete Math. **82** (1990), no. 2, 153–163, DOI 10.1016/0012-365X(90)90322-9. MR1057484

[Del01] Christophe Delaunay, *Heuristics on Tate-Shafarevitch groups of elliptic curves defined over $\mathbb{Q}$*, Experiment. Math. **10** (2001), no. 2, 191–196. MR1837670

[DH71] H. Davenport and H. Heilbronn, *On the density of discriminants of cubic fields. II*, Proc. R. Soc. Lond. Ser. A **322** (1971), no. 1551, 405–420. MR0491593

[Dha90] Deepak Dhar, *Self-organized critical state of sandpile automaton models*, Phys. Rev. Lett. **64** (1990), no. 14, 1613–1616, DOI 10.1103/PhysRevLett.64.1613. MR1044086

[DJ13] Joshua E. Ducey and Deelan M. Jalil, *Integer invariants of abelian Cayley graphs*, Linear Algebra Appl. **445** (2014), 316–325, DOI 10.1016/j.laa.2013.12.004. MR3151277

[Dur07] Richard Durrett, *Probability: Theory and Examples*, World Publishing Co., Beijing, 2007.

[EVW16] Jordan S. Ellenberg, Akshay Venkatesh, and Craig Westerland, *Homological stability for Hurwitz spaces and the Cohen-Lenstra conjecture over function fields*, Ann. of Math. (2) **183** (2016), no. 3, 729–786, DOI 10.4007/annals.2016.183.3.1. MR3488737

[EVW12] Jordan Ellenberg, Akshay Venkatesh, and Craig Westerland, Homological stability for Hurwitz spaces and the Cohen Lenstra conjecture over function fields, II. arXiv:1212.0923, 2012.

[FK06] Étienne Fouvry and Jürgen Klüners, *Cohen-Lenstra heuristics of quadratic number fields*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 4076, Springer, Berlin, 2006, pp. 40–55, DOI 10.1007/11792086_4. MR2282914

[FK07] Étienne Fouvry and Jürgen Klüners, *On the 4-rank of class groups of quadratic number fields*, Invent. Math. **167** (2007), no. 3, 455–513, DOI 10.1007/s00222-006-0021-2. MR2276261

[FW89] Eduardo Friedman and Lawrence C. Washington, *On the distribution of divisor class groups of curves over a finite field*, Théorie des nombres (Quebec, PQ, 1987), de Gruyter, Berlin, 1989, pp. 227–239. MR1024565

[Gab93a] Andrei Gabrielov, *Abelian avalanches and Tutte polynomials*, Phys. A **195** (1993), no. 1-2, 253–274, DOI 10.1016/0378-4371(93)90267-8. MR1215018

[Gab93b] Andrei Gabrielov, *Avalanches, sandpiles and Tutte decomposition*, The Gel′fand Mathematical Seminars, 1990–1992, Birkhäuser Boston, Boston, MA, 1993, pp. 19–26. MR1247281

[Gar12] Derek Garton, *Random matrices and Cohen-Lenstra statistics for global fields with roots of unity*, ProQuest LLC, Ann Arbor, MI, 2012. Thesis (Ph.D.)–The University of Wisconsin–Madison. MR3078415

[Ger87a] Frank Gerth III, *Densities for ranks of certain parts of p-class groups*, Proc. Amer. Math. Soc. **99** (1987), no. 1, 1–8, DOI 10.2307/2046260. MR866419

[Ger87b] Frank Gerth III, *Extension of conjectures of Cohen and Lenstra*, Expo. Math. **5** (1987), no. 2, 181–184. MR887792

[Gir84] V. L. Girko, *The circular law* (Russian), Teor. Veroyatn. Primen. **29** (1984), no. 4, 669–679. MR773436

[Gir04] V. L. Girko, *The strong circular law. Twenty years later. II*, Random Oper. Stoch. Equ. **12** (2004), no. 3, 255–312, DOI 10.1163/1569397042222477. MR2085255

[GT06] F. Götze and A. N. Tikhomirov, *Limit theorems for spectra of random matrices with martingale structure* (English, with Russian summary), Teor. Veroyatn. Primen. **51** (2006), no. 1, 171–192, DOI 10.1137/S0040585X97982268; English transl., Theory Probab. Appl. **51** (2007), no. 1, 42–64. MR2324173

[GT10] Friedrich Götze and Alexander Tikhomirov, *The circular law for random matrices*, Ann. Probab. **38** (2010), no. 4, 1444–1491, DOI 10.1214/09-AOP522. MR2663633

[HB94a] D. R. Heath-Brown. *The size of Selmer groups for the congruent number problem, II.* **118** (1994). preprint version, http://eprints.maths.ox.ac.uk/154/.

[HB94b] D. R. Heath-Brown, *The size of Selmer groups for the congruent number problem. II*, Invent. Math. **118** (1994), no. 2, 331–370, DOI 10.1007/BF01231536. With an appendix by P. Monsky. MR1292115

[HLM+] Alexander E. Holroyd, Lionel Levine, Karola Mészáros, Yuval Peres, James Propp, and David B. Wilson, *Chip-firing and rotor-routing on directed graphs*, In and out of equilibrium. 2, Progr. Probab., vol. 60, Birkhäuser, Basel, 2008, pp. 331–364, DOI 10.1007/978-3-7643-8786-0_17. MR2477390

[HR07] Christopher J. Hillar and Darren L. Rhea, *Automorphisms of finite abelian groups*, Amer. Math. Monthly **114** (2007), no. 10, 917–923. MR2363058

[HST06] Matthew D. Horton, H. M. Stark, and Audrey A. Terras, *What are zeta functions of graphs and what are they good for?*, Quantum graphs and their applications, Contemp. Math., vol. 415, Amer. Math. Soc., Providence, RI, 2006, pp. 173–189, DOI 10.1090/conm/415/07868. MR2277616

[KK01] Jeff Kahn and János Komlós, *Singularity probabilities for random matrices over finite fields*, Combin. Probab. Comput. **10** (2001), no. 2, 137–157, DOI 10.1017/S096354830100462X. MR1833067

[KKS95] Jeff Kahn, János Komlós, and Endre Szemerédi, *On the probability that a random ±1-matrix is singular*, J. Amer. Math. Soc. **8** (1995), no. 1, 223–240, DOI 10.2307/2152887. MR1260107

[KL75] I. N. Kovalenko and A. A. Levitskaya, *Limiting behavior of the number of solutions of a system of random linear equations over a finite field and a finite ring* (Russian), Dokl. Akad. Nauk SSSR **221** (1975), no. 4, 778–781. MR0380957

[KLS86] I. N. Kovalenko, A. A. Levitskaya, and M. N. Savchuk, *Izbrannye zadachi veroyatnostnoi kombinatoriki* (Russian), "Naukova Dumka," Kiev, 1986. MR899073

[Koz66] M. V. Kozlov, *On the rank of matrices with random Boolean elements*, Sov. Math. Dokl. **7** (1966), 1048–1051. MR0224119

[Kom67] J. Komlós, *On the determinant of* (0, 1) *matrices*, Studia Sci. Math. Hungar. **2** (1967), 7–21. MR0221962

[Kom68] J. Komlós, *On the determinant of random matrices*, Studia Sci. Math. Hungar. **3** (1968), 387–399. MR0238371

[L97] Criel Merino López, *Chip firing and the Tutte polynomial*, Ann. Comb. **1** (1997), no. 3, 253–259, DOI 10.1007/BF02558479. MR1630779

[Lor89] Dino J. Lorenzini, *Arithmetical graphs*, Math. Ann. **285** (1989), no. 3, 481–501, DOI 10.1007/BF01455069. MR1019714

[Lor90] Dino J. Lorenzini, *A finite group attached to the Laplacian of a graph*, Discrete Math. **91** (1991), no. 3, 277–282, DOI 10.1016/0012-365X(90)90236-B. MR1129991

[Lor00] Dino Lorenzini, *Arithmetical properties of Laplacians of graphs*, Linear Multilinear Algebra **47** (2000), no. 4, 281–306, DOI 10.1080/03081080008818652. MR1784872

[Lor08] Dino Lorenzini, *Smith normal form and Laplacians*, J. Combin. Theory Ser. B **98** (2008), no. 6, 1271–1300, DOI 10.1016/j.jctb.2008.02.002. MR2462319

[LP10] Lionel Levine and James Propp, *What is ... a sandpile?*, Notices Amer. Math. Soc. **57** (2010), no. 8, 976–979. MR2667495

[Mac69] Jessie MacWilliams, *Orthogonal matrices over finite fields*, Amer. Math. Monthly **76** (1969), 152–164. MR0238870

[Mal08] Gunter Malle, *Cohen-Lenstra heuristic and roots of unity*, J. Number Theory **128** (2008), no. 10, 2823–2835, DOI 10.1016/j.jnt.2008.01.002. MR2441080

[Mal10] Gunter Malle, *On the distribution of class groups of number fields*, Experiment. Math. **19** (2010), no. 4, 465–474, DOI 10.1080/10586458.2010.10390636. MR2778658

[Map10] Kenneth Maples, *Singularity of random matrices over finite fields*. arXiv:1012.2372[math], December 2010.

[Map13] Kenneth Maples, *Cokernels of random matrices satisfy the Cohen-Lenstra heuristics*, 2013. arXiv:1301.1239.

[Meh67] M. L. Mehta, *Random Matrices and the Statistical Theory of Energy Levels*, Academic Press, New York-London, 1967. MR0220494

[Ngu12] Hoi H. Nguyen, *Inverse Littlewood-Offord problems and the singularity of random symmetric matrices*, Duke Math. J. **161** (2012), no. 4, 545–586, DOI 10.1215/00127094-1548344. MR2891529

[NW11] Serguei Norine and Peter Whalen, *Jacobians of nearly complete and threshold graphs*, European J. Combin. **32** (2011), no. 8, 1368–1376, DOI 10.1016/j.ejc.2011.04.003. MR2838022

[PZ10] Guangming Pan and Wang Zhou, *Circular law, extreme singular values and potential theory*, J. Multivariate Anal. **101** (2010), no. 3, 645–656, DOI 10.1016/j.jmva.2009.08.005. MR2575411

[Pas72] L. A. Pastur, *The spectrum of random matrices* (Russian, with English summary), Teoret. Mat. Fiz. **10** (1972), no. 1, 102–112. MR0475502

[Sho10] Farbod Shokrieh, *The monodromy pairing and discrete logarithm on the Jacobian of finite graphs*, J. Math. Cryptol. **4** (2010), no. 1, 43–56, DOI 10.1515/JMC.2010.002. MR2660333

[TV06] Terence Tao and Van Vu, *On random* ± 1 *matrices: singularity and determinant*, Random Structures Algorithms **28** (2006), no. 1, 1–23, DOI 10.1002/rsa.20109. MR2187480

[TV07] Terence Tao and Van Vu, *On the singularity probability of random Bernoulli matrices*, J. Amer. Math. Soc. **20** (2007), no. 3, 603–628, DOI 10.1090/S0894-0347-07-00555-3. MR2291914

[TV08] Terence Tao and Van Vu, *Random matrices: the circular law*, Commun. Contemp. Math. **10** (2008), no. 2, 261–307, DOI 10.1142/S0219199708002788. MR2409368

[TV10] Terence Tao and Van Vu, *Random matrices: universality of ESDs and the circular law*, Ann. Probab. **38** (2010), no. 5, 2023–2065, DOI 10.1214/10-AOP534. With an appendix by Manjunath Krishnapur. MR2722794

[Ver11] Roman Vershynin, *Invertibility of symmetric random matrices*, Random Structures Algorithms **44** (2014), no. 2, 135–182, DOI 10.1002/rsa.20429. MR3158627

[Wag00] David G. Wagner. The critical group of a directed graph. *arXiv:math/0010241*, October 2000.

[Wig58] Eugene P. Wigner, *On the distribution of the roots of certain symmetric matrices*, Ann. of Math. (2) **67** (1958), 325–327. MR0095527

Department of Mathematics, University of Wisconsin–Madison, 480 Lincoln Drive, Madison, Wisconsin 53705, and American Institute of Mathematics, 360 Portage Avenue, Palo Alto, California 94306-2244

E-mail address: mmwood@math.wisc.edu